Body Sensor Network

Case study title: Body Sensor Network

Description

The SA-BSN is an exemplar of a healthcare application implemented in ROS [1]. The goal of the SA-BSN is to detect emergencies by continuously monitoring the patient’s health status. Furthermore, the SA-BSN is equipped to adapt itself in order to maintain the desired QoS levels with minimal human intervention, while accounting for classes of uncertainty.

A range of vital signs is periodically collected from the patient through a set of distributed sensors: electrocardiograph sensor (ECG) for heart rate and electrocardiogram curve; a pulse oximeter (SaO2) for measuring blood oxygen saturation; a thermometer (TEMP), that collects the body temperature in Celsius; a sphygmomanometer for measuring and systolic arterial blood pressure (ABP); there is also a Glucose sensor for measuring blood glucose levels. The collected data is then forwarded to the Central Hub: a component in the Managed System to fuse the vital signs and classify the overall health situation of the patient into low, moderate, or high risk status. As a self-adaptive system, the BSN has the Managing System module, which is responsible for continuously assuring the fulfillment of the desired QoS attributes related to the values of reliability and battery consumption (i.e. cost).

For the evaluation of the quality of the adaptation the BSN uses control theory metrics following the terminology proposed by Camara et al. [2]. The chosen QoS constraint is attributed to a setpoint, which is set by the user before the system execution. For example, if the concerned QoS attribute is the reliability, one could set it to 95%, within an acceptable error range. This is called setpoint tracking, which can be measured by the steady-state error (SSE) metric.

Moreover, while trying to meet its requirements, the system is prone to a range of uncertainties. Thus, the controller is activated to mitigate the effects of unexpected events in quality attributes. Such uncertainties can be depicted in three distinctive scenarios. The first scenario, S1, focuses on uncertainties related to the overflow of sensed data into the Central Hub queue and also to the possible data uncertainties in sensors, which are related to the reliability of the system. The second scenario, S2, focuses on the uncertainty related to the operational frequencies of the components, which can lead to a battery consumption that exceeds what is needed to satisfy the requirements. In the third scenario, S3, depending on the patient profile, the operator may not want to use certain sensors; with fewer components to manage, less uncertainty in the system is expected and, consequently, a more stable adaptation process.

[1] M. Quigley, K. Conley, B. Gerkey, J. Faust, T. Foote, J. Leibs, R. Wheeler, and A. Y. Ng, “ROS: an open-source robot operating system,” in ICRA workshop on open source software, vol. 3, no. 3.2. Kobe, Japan, 2009, p. 5.

[2] J. Camara, A. V. Papadopoulos, T. Vogel, D. Weyns, D. Garlan, S. Huang, and K. Tei, “Towards bridging the gap between control and self-adaptive system properties,” ser. SEAMS ’20. New York, NY, USA: Association for Computing Machinery, 2020, p. 78–84.

Stage of Development (Technical contributor)

Currently there is the BSN prototype implemented in ROS. Additionally, it has been integrated with sensors like thermometer and SPO_2 running in Arduino Leonardo and embedded in a Raspberry Pi 4GB board.

Expert info

Stakeholder names	Expertise
TS-1	engineer and safety analyst
TS-2	Engineer/Goal Modelling
N-TS-1	Social/Moral Psychology
N-TS-2	Moral Psychology, Law

Normative requirements

1. Normative requirements in natural language

Normative requirements in natural language, in blue the corrected requirements after using N-Tool.

rule id	rule	impact	label(s) (social, legal, ethical, empathetic, or cultural)	stakeholder expertise	authors identifiers
1	When the patient is sleeping, the BSN must keep track of the patient vital signs, despite	-A +T +S	empathetic	engineer and safety analyst	TS-1

	potential patient’s discomfort while sleeping ● unless it can be removed by liable care giver due to patient’s discomfort	-N			
1bis	When the patient is sleeping, update the patient status to sleeping, and deactivate functions that requires communicating with the patient, only keep monitoring				
1bis2	When the patient is sleeping, then can not measure discomfort from patient directly unless sleeping pattern changed and it is not first week				
2	When the patient is performing day-to-day activities, the monitored vital signs should still be accurate (steady-state error should not change) ● Unless the patient's sensed signs become impaired by the patient's sweat or body detachment due to patient's movements AND alternative sensors are deployed on the patient body to avoid sensor read imprecision.	+A +T +S	legal	engineer and safety analyst, Engineer/Goal Modelling	TS-1, TS-2
3	When the patient is in the bathroom the vital signs should be monitored ● Unless the equipment is not waterproof and the monitored patient is provided with a fall alert system necklace pendant. ● Unless patient does not allow vital signs to be disclosed in this context.	+A +S +P	ethical, empathetic,	engineer and safety analyst	TS-1

4	When the patient is outside home, the geographical location should not be disclosed ● unless the device can communicate with the patient regularly. ● unless there are authorized parties to track the patient ● unless an emergency is accurately detected.	+P +E	legal, ethical	engineer and safety analyst	TS-1
5	When there is an unexpected number of vital sign and there are message processing delays, then adjust the Central Hub service time rate	+T +E	legal	Engineer/Goal Modelling	TS-2
6	When there is an uncertain sampling size and uncertain mean time to failure, or battery consumption is high, then adjust the sensors' sampling rate	+T +E	legal	Engineer/Goal Modelling	TS-2
7	When an emergency is confirmed, call the caregiver. If severity is moderate. Call the caregiver and an ambulance if the severity is high.	+S +T -P -A	ethical, empathetic	Engineer/Goal Modelling	TS-2
8	If an anomaly in vital signals is detected, ensure that they are not caused by circumstantial conditions. - Confirm with the user if all sensors are properly placed. - Confirm if the user is not performing any unusual physical activity (e.g., strenuous exercise)	+SR +A	social	Social/Moral Psychology	N-TS-1
9	If an anomaly in vital signals is detected but not caused by sensor malfunction, misplacement, or unusual activity, inform the user about it. - If user does not respond to this information in any way, notify their	+SR +S +B	Social Ethical	Social/Moral Psychology	N-TS-1

	emergency contact. - If emergency does not answer, call medical help.				
10	In first interaction with the user, get informed consent for collecting, recording, and sending their information to other parties.	+SR +A	Social Ethical Legal	Social/Moral Psychology	N-TS-1
11	In first interaction with the user, inform them of the purposes of using this technology. - Ask them for an emergency contact and inform them that the emergency contact can be contacted if the sensors detect anomalies in their vital signs. - Inform them about what will happen in case the sensors malfunction and they do not respond.	+SR +S	social ethical	Social/Moral Psychology	N-TS-1
12	If data collected is no longer relevant or necessary, do not store it. If data is still required for training purposes, de-identify it - User must give clear and informed consent for their identified data to be stored and accessed	+S +T +P	Social Legal	Psychology Law	N-TS-2
13	If user at any time wishes to stop/opt out of use of BSN for monitoring vital signs, the process to do so must be quick and easy - Unless risk to user from removal of sensors outweighs autonomy concern - If patient wants to remove sensors, alert the caregiver - Sensors must not be removed unless caregiver gives explicit	-A +S +PH +B +N +P	Social Legal Empathetic	Psychology Law	N-TS-2

	instructions to do so				
14	User health history, demographics, and geographical location must be used to inform/calibrate BSN signal categorization so that system does not overly and unnecessarily interfere with user's life or cause unnecessary distress - Signals must be compared to a healthy adult from the user's socio-ethnic group - (e.g., Populations living in mountainous locations (for example) naturally possess higher blood oxygen saturation levels without cause for concern)	+S +B +N +CS +SR	Cultural Social Empathetic	Psychology Law	N-TS-2
15	BSN should allow for storing of user data only for a buffer period of time (pre-specified)	+P	Legal		
15bis	All data collected must be de-identified				
16	Hardware must not unreasonably interfere with user's cultural and religious activities - Ask the user for their consent prior to fitting BSN	+A +PH +SR	Social Cultural Legal Empathetic Ethical	Psychology Law	N-TS-2
17	User must have other avenues to contact emergency services, even in cases where BSN is not recording anomalies in vital signs	+S +A +B	Social Legal	Psychology Law	N-TS-2
18	As soon as system is setup, user and caregiver should be asked about the level of risk of the patient. - Depending on this level	+S +A +T			All stakeholders

	of risk, low quality information from the sensors could be interpreted as either a health hazard or a delay in communication.				
19	When the user requests to remove the sensors and the patient is responsible (autonomous) enough, then a reliable caregiver must remove it (reliable caregiver has the permission to remove the sensor to the specific patient) .				
MAIN NEGATIVE CONCERN					
1	Patient should not be able to remove sensors by himself.	-A +T +S -N	empathetic	engineer and safety analyst	All stakeholders
2	Every time sensors are adjusted, ask the patient for their level of comfort. If their level of comfort is below a certain threshold, adjust sensors until the patient feels comfortable.				
3	The patient's privacy should be respected as much as possible. Patient should be able to select when they want a time out from the sensors. Patient should always be informed that their health monitoring will be decreased when they do it.				
3	If the patient does not want to wear the sensors due to privacy, the system should check in with the patient (via notifications). - The system should also inform the user of the risks and tradeoffs between privacy and health as soon as they remove the sensors.				

5	System should not shut down if there is a flush of information (more than the system can handle).				
6	As soon as system is setup, user and caregiver does not ask about the level of risk of the patient.				
PURPOSE					
1	User should be able to not disclose their geographic location while outdoors				
2	BSN must be able to call a caregiver in case of an emergency				
3	BSN system must be able to comply with a user's cultural and religious activities				
4	BSN must be able to delete data when it is no longer necessary and is not being used for training				
5	BSN must be able to anonymize data when it is being used				
6	BSN must be able to call an ambulance when the risk level is greater than moderate				
7	BSN must be able to inform the user when an anomaly is detected while tracking vitals				
Impact keys: A = autonomy, PH = psychological health (non-maleficence), P = privacy, E = explainability, T = transparency, CS = cultural sensitivity, SR = social requirement, B 'beneficence' (doing good), N 'non-maleficence' (preventing/avoiding harm), and S 'safety'. ''+" and "-" for positive and negative impacts respectively.					

1. **Rules in the SLEEC DSL**

The stakeholders corrections after analyzing the well-formedness of the rules using our N-Tool are commented and in blue.

```
def_start
        // BSN actions
        event HideGeographicLocation
        event ConfirmSensorPlacement
        event ConfirmUsersActivities
        event AdjustServiceTimerate
        event AdjustSamplingRate
        event CalibrateBSN
        event EnsureHardwareCompliance
        // Related to contacts and emergency
        event EmergencyConfirmed
        event CallAmbulance
        event ObtainEmergencyContact
        // Related to BSN and human interactions
        event MeetingUser
        event ObtainUserConsentForData
        event ObtainUserConsentForSensors
        event InformUser
        event TrackVitals               // With assumption that this is being done accurately
        event InformBSNPurposeAndResponseProtocol
        event CallCaregiver
        event EnsureEasyStopping
        event RemoveSensors
        event CaregiverCanDeactivate
        // Related to data
        event DataCollected
        event DeleteData
        event AnonymizeData
        // Patient actions
        event patientOutdoors
        event patientAsleep
        event patientDoingChores
        event patientBathing
        event userWantsToRemoveSensors
        event userCanCallEmergency
        event adjustSensors
        event userWantsTimeout
        event systemShutDown
        event obtainRiskLevel
        //******** Resolve concern c2 (ADD event)
        event UserRequestRemoveSensor
        //*************************************************
        measure patientDiscomfort: scale{low, moderate, high}
        measure riskLevel: scale{low, moderate, high}
        measure batteryConsumption: scale{low, moderate, high}
        measure numUsersKnown: boolean
        measure numSampleKnown: boolean
        measure canDeactivate: boolean
```

```
    measure patientIsHome: boolean
    measure signsImpaired: boolean
    measure signsDetached: boolean
    measure isWaterproof: boolean
    measure hasFallAlertPendant: boolean
    measure allowsBathroomTracking: boolean
    measure canCommunicateRegularly: boolean
    measure authorizedParties: boolean
    measure emergencyDetected: boolean
    measure messageOnTime: boolean
    measure alternateSensorsDeployed: boolean
    measure timeToFailureKnown: boolean
    measure anomalyDetected: boolean
    measure unusualActivity: boolean
    measure sensorMalfunction: boolean
    measure sensorMisplacement: boolean
    measure userResponds: boolean
    measure caregiverResponds: boolean
    measure dataNeededForTraining: boolean
    measure userWantsToStop: boolean
    measure caregiverConsent: boolean
    measure seeHealthHistory: boolean
    measure seeDemographics: boolean
    measure seeLocation: boolean
    measure accurateHealthComparison: boolean
    //****** Resolve concern add two measures
    // comment canDeactivate
    measure canPatientDeactivate: boolean
    measure canCaregiverDeactivate: boolean
    //*************************************************

    constant autonomyConcern
    constant bufferPeriod
def_end
rule_start
    // Natural language rule 1
    // Track no matter what comfort is, unless it is medium or high and the caregiver can deactivate
    Rule1 when patientAsleep and {{patientDiscomfort} = low or {patientDiscomfort} = medium or
{patientDiscomfort} = high} then trackVitals
        unless {canDeactivate} and {{patientDiscomfort > low}} then caregiverCanDeactivate

    // Natural language rule 2
    Rule2 when patientDoingChores and {patientIsHome} then trackVitals
        unless {{signsImpaired} or {signsDetached}} and {alternateSensorsDeployed}

    // Natural language rule 3
    Rule3 when patientBathing then trackVitals
        unless {{not {isWaterproof}} and {hasFallAlertPendant}} or {not {allowsBathroomTracking}}

    // Natural language rule 4
    Rule4 when patientOutdoors and {not {patientIsHome}} then hideGeographicLocation
        unless {canCommunicateRegularly}
        unless {authorizedParties}
        unless {emergencyDetected}
```

```
// Natural language rule 5
Rule5 when trackVitals and {not {messageOnTime}} and {not {numUsersKnown}}
then adjustServiceTimerate

Rule5_1 when trackVitals and {not {messageOnTime}} and {not {numUsersKnown}}
then not systemShutDown

// Natural language rule 6
Rule6 when trackVitals and {{not {timeToFailureKnown}} and {not {numSampleKnown}}}
or {{batteryConsumption} = high} then adjustSamplingRate

Rule6_1 when trackVitals and {{not {timeToFailureKnown}} and {not {numSampleKnown}}}
or {{batteryConsumption} = high} then not systemShutDown

// Natural language rule 7 part 1
// Because we can call for help whenever there is an emergency
Rule7 when emergencyConfirmed then callCaregiver

// Natural language rule 7 part 2
// But only inform caregiver when the risk level is medium or high
Rule7_1 when emergencyConfirmed and {{riskLevel >= moderate} then callAmbulance

// If an anomaly in vital signals is detected ensure that they are not caused by circumstantial conditions.
// Confirm with user all sensors are properly placed
Rule8 when trackVitals and {anomalyDetected} then confirmSensorPlacement

// Confirm if the user is not performing any unusual physical activity
Rule8_1 when trackVitals and {anomalyDetected} then confirmUsersActivities

// If an anomaly in vital signals is detected but not caused by sensor malfunction, misplacement, or unusual activity, inform the user about it.
Rule9 when trackVitals and {anomalyDetected} and {not {unusualActivity}} and {not {sensorMalfunction}}
and {not {sensorMisplacement}} then informUser

// If user does not respond to this information in any way, notify their emergency contact.
Rule9_1 when informUser and {not {userResponds}} then callCaregiver

// If emergency does not answer, call medical help.
Rule9_2 when callCaregiver and {not {caregiverResponds}} then callAmbulance

Rule10 when meetingUser then obtainUserConsentForData
// In first interaction with the user, inform them of the purposes of using this technology.
// inform them that the emergency contact can be contacted if the sensors detect anomalies in their vital signs.
// Inform them about what will happen in case the sensors malfunction and they do not respond
Rule 11 when meetingUser then informBSNPurposeAndResponseProtocol

// Ask them for an emergency contact
Rule 11_1 when meetingUser then obtainEmergencyContact

Rule 12 when dataCollected and {not {dataNeededForTraining}} then deleteData
        unless {dataNeededForTraining} then anonymizeData
```

```
    Rule 13 when trackVitals and {userWantsToStop} then ensureEasyStopping
        unless {{riskLevel} > autonomyConcern}
        // If risk to user from removal is low, then alert caregiver
        otherwise callCaregiver

    // Do not remove sensors without explicit consent from caregiver to do so
    Rule13_1 when userWantsToRemoveSensors and {not {caregiverConsent}} then not removeSensors

    Rule13_2 when userWantsToRemoveSensors then informUser

    Rule13_3 when userWantsTimeout then informUser

    // Inform/calibrate BSN signal so that the system doesn't overly interfere or cause stress
    Rule14 when calibrateBSN and {seeHealthHistory} and {seeDemographics} and {seeLocation} and
{accurateHealthComparison} then trackVitals

    Rule15 when dataCollected then deleteData within bufferPeriod

    //****** Resolve concern c8 (ADDED one rule (15bis))
     // Uncomment rulle Rule15bis
    //Rule15bis when DataCollected then AnonymizeData
    //**********************************************************************

    // Hardware must not unreasonably interfere with user's culture and religious acts
    Rule16 when meetingUser then ensureHardwareCompliance

    // Ask user for consent prior to fitting BSN
    Rule16_1 when meetingUser then obtainUserConsentForSensors

    Rule17 when trackVitals then userCanCallEmergency

    Rule18 when calibrateBSN then obtainRiskLevel

    //****** Resolve c2 (ADD a rule)
    // Uncomment Rule19
    // Rule19 when UserRequestRemoveSensor and {canCaregiverDeactivate} then CaregiverCanDeactivate
    //**********************************************************************
    //****** Resolve c9 (ADD a rule Rule19b)
    // Uncomment Rule19b
    // Rule19b when UserWantsToRemoveSensors and {canPatientDeactivate} then CaregiverCanDeactivate
    //**********************************************************************
rule_end

// Security, autonomy, legal, cultural, privacy, safety.
concern_start
    // Patient should not be able to remove sensors by himself.
    C1 when userWantsToRemoveSensors and {not {caregiverConsent}} then removeSensors

    C2 when trackVitals and {canDeactivate} and {{patientDiscomfort} > low} then not caregiverCanDeactivate

    // The patient's privacy should be respected as much as possible. Patient should be able to select when they
want a time out from the sensors. Patient should always be informed that their health monitoring will be decreased
when they do it.
    C3 when userWantsTimeout then not informUser
```

```
	// If the patient does not want to wear the sensors due to privacy, the system should check in with the patient (via notifications). The system should also inform the user of the risks and tradeoffs between privacy and health as soon as they remove the sensors.
	C4 when userWantsToRemoveSensors then not informUser

	// System should not shut down if there is a flush of information (more than the system can handle).
	C5 when trackVitals and {not {messageOnTime}} and {not {numUsersKnown}} then systemShutDown

	// As soon as system is setup, user and caregiver does not ask about the level of risk of the patient.
	C6 when calibrateBSN then not obtainRiskLevel
concern_end
purpose_start
// The purpose is to monitor a patient's health respecting their autonomy, safety, cultural differences, and privacy while protecting the user against security threats.
	// Autonomy - User should be able to not disclose their geographic location while outdoors
	P1 exists hideGeographicLocation and {not {patientIsHome}}

	// Safety - BSN should be able to call a caregiver in case of an emergency
	P2 exists callCaregiver while emergencyConfirmed

	// Cultural difference
	P3 exists ensureHardwareCompliance

	// Privacy - BSN should be able to delete data when it is no longer necessary
	P4 exists deleteData and {not {dataNeededForTraining}}

	// Privacy - BSN should be able to anonymize data when it is being used
	P5 exists anonymizeData and {dataNeededForTraining}

	// Protect against threats
	P6 exists callAmbulance and {riskLevel >= moderate}

	// BSN should be able to inform user when an anomaly is detected while tracking vitals
	P7 exists informUser and {anomalyDetected} while trackVitals
purpose_end
```