A Safe and Interoperable Distributed Alarm Notification System for PoC Medical Devices using IEEE 11073 SDC

Martin Kasparick[1], Frank Golatowski[1], and Dirk Timmermann[1]

***Abstract*— The flood of alarms produced by Point-of-Care (PoC) medical devices in intensive care units (ICUs) and operating rooms (ORs) is a crucial issue of today's hospitals. Alarm fatigue and desensitization leads to the death of patients, noise worsens the patient's recovery process and causes burn-out syndromes of caregivers, etc. Much research has been done in the last years to reduce false alarms and noise with smart and intelligent alarm systems. However, the situation has not improved. The developed systems are not used in the field, likely due to the "better-safe-than-sorry" mentality. Thus, we state that the first step to address alarm related problems is a safe and distributed system for alarm notifications. Therefore, we present mechanisms to generate alarm notifications safely at the place where they are needed by the caregivers, that is not necessarily the bedside. Our approach holds safety, risk management, and approval requirements. We use the new IEEE 11073 Service-oriented Device Connectivity (SDC) standard family. This ensures a safe interoperability of heterogeneous devices from multiple manufacturers, which is a major technical innovation, and makes the proposed system ready for future extensions like intelligent, computer-aided assistive systems. We therefore state that our mechanisms have a high potential to be used in the field and to improve clinical problems related to alarm notification systems. A demonstrator has been implemented for the proof of concept.**

I. Introduction

Alert management is one of the most important issues for patients and caregivers in hospitals, especially in intensive care units (ICUs) and operating rooms (ORs). Depending on the consulted study, results vary between 80% and 99% clinically non-relevant alarms [1], [2], [3]. Considering that more than one (1.2 [2]) alert occurs per minute during the perioperative phase or an average of 2.1 alarms occur per hour and patient at an ICU [4], this results in an immense workload for caregivers and leads to the problem of alarm fatigue [3]. Alarm hazards are in the leading positions on the ECRI Institute top 10 list of health technology hazards [3], [5]. This even leads to the death of patients, e.g., caused by inadvertently turned-off alarms.

Furthermore, the noise in hospital environments is a big problem. Alarm volumes of up to 80 db(A) [1], [4] harm patients and caregivers. Studies show that noise causes significant stress leading to sleep deprivation of patients, which badly influences the immune response and nervous system activity and can even cause psychosis [1], [2]. For nurses the permanent noise increases the risk of burn-out syndromes and reduces the concentration during their work [1], [2].

*This work was not supported by any organization.

[1]Author is with the Institute of Applied Microelectronics and Computer Engineering, University of Rostock, 18119 Rostock, Germany firstname.lastname@uni-rostock.de

As research during the recent years has not lead to significant changes in the clinical reality [2], we propose mechanisms for safe and distributed alarm notifications in this paper. Distributed alarm systems allowing the alarm notification at the current location of the caregiver, that is not necessarily at the bedside, have several advantages. For example, reduced noise for the patient; reduced noise for caregivers as mobile, personalized devices can be adjusted more accurately; lower workload for the caregivers, e.g., due to shorter walking distances and the possibility of getting deeper information about alarm reasons from interoperable networked devices; allowing centralized monitoring stations for a better care coordination; etc. Additionally, the proposed systems can act as a base technology for further development and realization of intelligent, computer-aided alarm systems.

Our work is based on the new service-oriented approach of manufacturer-independent medical device interoperability defined in the new IEEE 11073 SDC family of standards.

II. State of the Art

Based on an analysis of the state of the art, we derive the need for safe, distributed, and manufacturer-independent alarm notification systems.

A. Alarm Notification Systems

There are patents and systems available on the market realizing manufacturer-dependent solutions for distributed alarm notification systems based on proprietary and isolated protocols. Safe, comprehensive, and flexible systems using standardized interconnection are not available.

Lots of research and development has been done in the field of alarm management for ICU and OR in the last years, comprehensively reviewed and surveyed for example in [1], [2], [3], [4]. High effort has been made to address the problems of high false positive rate of medical alarms, alarm audibility and identification, noise caused by alarm notifications, alarm fatigue, desensitization, etc. Under the headlines of *smart* or *intelligent alarm systems* there are plenty of approaches: Cross checking alarms of different sources like heartrate from electrocardiogram (ECG) and pulse oximetry; alert setting modification according to a phase analysis of the surgical procedure or other patient contextual information; statistical methods for signal extraction and filtering; root cause analysis; trend monitoring; etc. Some research projects use complex methods of artificial intelligence, like neuronal networks, fuzzy logic, or Bayesian networks. However, there are even very simple approaches like using a time delay: An alarm is only triggered if the condition, like an exceeded

threshold, is fulfilled for a certain period of time. Studies have shown the effectiveness of this approach.

Although there are plenty of convincing approaches, the false alarm rate has not decreased in clinical reality during the last years [2]. The usage of *smart and intelligent alarms* lags behind the general advancement of medical devices [6]. Liability concerns as well as manufacturers' business factors seem to be reasons [6]. The current "better-safe-than-sorry" mentality of manufacturers and approval authorities implies that plenty of false alarms are rather accepted than the possibility to miss a valid alarm [2].

Therefore, we state that the first step to encounter the alert problem is a safe, manufacturer-independent, and standardized interconnection of medical devices as basis for a safe distributed alarm notification system. This approach is also supported by conclusions and needs for research figured out by the mentioned surveys. As a basic problem, interoperability is almost unavailable for medical devices in ICU, OR, and the whole hospital. Manufacturers have treated interoperability with low priority and as a costly endeavor on the one hand, and the users have not understood and appreciated the need and benefits on the other hand [7].

Borowski et al. [1] figure out that networked alarm devices could have a positive impact on the amount of alarms. Thus, the current state of neither standardized nor interconnected medical devices has to be resolved. Interoperability based on standardized and certified interfaces is necessary. Especially the patient's safety has to be addressed for networked and interoperable systems, as the required reliability is very high and liability issues have to be considered for alarm systems [1]. Cvach [3] underlines the importance of adjunct devices for alert notifications to improve alarm audibility and identification. Especially, she points up the need for further research on alarm notifications based on wireless technology [3]. Konkani et al. [4] analyze the need of secondary or third-party alarm notification systems mediating between patient and caregivers.

It can be concluded that there is a strong need for a safe, distributed, and manufacturer-independent alarm notification system based on standardized communication interfaces and interoperability mechanisms holding liability issues. Konkani et al. state that in current third-party systems every participant is a single point of failure (SPOF), that a failure of any device causes the failure of the whole system [4]. In contrast, the mechanisms proposed in this paper describe a completely distributed alarm notification approach without SPOFs and thus being suitable also for wireless communication.

B. IEEE 11073 SDC

The new IEEE 11073 standard family for Service-oriented Device Connectivity (SDC) defines an emerging and promising technology for safe, interoperable, and manufacturer-independent interconnection of networked Point-of-Care (PoC) medical devices. The family comprises three standards. The Medical Devices Communication Profile for Web Services (MDPWS) defined in IEEE 11073-20702 describes the data transport mechanisms, based on the idea of a Service-Oriented Architecture (SOA) [8]. The Domain Information & Service Model (IEEE P11073-10207) address the structural interoperability. It defines the way medical devices describe their capabilities and state as well as the provided services to interact with the device [9]. Additionally, the allover architecture and the binding between the two previously mentioned standards is defined in IEEE P11073-20701. While the first artifact has passed the standardization process in 2016, the latter two are currently in the process of standardization.

III. Requirements for Safe and Distributed Alarm Notification Systems

A distributed alarm notification system has to fulfill several requirements. They can be derived from the needs for research as analyzed in Sec. II and from safety issues, like defined in IEC 60601. On the one hand, there are requirements that have to be fulfilled to allow networked medical devices to notify alarms being generated at another medical device. On the other hand, there are requirements arising from the device monitoring the alert condition and primarily producing the alert notification (alarm producer).

Requirement 1: The alarm producer has to make all information available that are necessary for the remote alarm notifiers (RANs), like alert condition presence, alert manifestation, etc. Manufacturer-interoperability and semantical interpretability have to be ensured.

Requirement 2: The system has to be suitable for multiple alarm producers and several remote alarm notifying devices.

Requirement 3: The alarm producer has to be able to determine whether other devices are ready to generate the alarm notification.

Requirement 4: The alarm producer has to be able to observe that the alert is generated correctly.

The first requirement serves as basis for a distributed, open, manufacturer-independent, and interoperable device solutions As medical device ensembles are complex and multiple patients have to be treated by multiple caregivers at the same time, requirement two is needed. The third and fourth requirements arise from the risk management of the alarm producer. The alarm producer can only deactivate its own alarm notification if it can be sure that at least one other suitable device generates the alarm notification in the correct way. The system is designed for networked medical device systems and especially wireless connections will be used for distributed alarm notification systems. Thus, robustness against connection loss, lost information, jitter, etc., has to be ensured. In the case of any unintended behavior of the RAN, the alarm producer has to be able to generate the alarm notification on its own if this is necessary according to the risk management.

We use the SOA-based IEEE 11073 SDC standard family to cope with Requirement 1 – 4. Thus, an additional requirement arises, to clearly distinguish the SOA service provider and service consumer role. In addition to the alert functionality, alarm producers will typically provide further information, like the basic measurement leading to the alarm. Common alarm producers are patient monitors providing plenty of measurements and alarms. Central ICU or OR

dashboards or even mobile devices like smart phones will act as RANs. From the SOA point of view, they act logically as service consumers. From the aim not to increase the complexity of both components, alarm producer and RAN, and additionally from the basic idea of the SOA to separate between service consumer and service provider, the fifth requirement is derived:

Requirement 5: Safety mechanisms shall not require to extend the basic roles of alarm producer (service provider) and RAN (service consumer).

IV. Mechanisms for Safe and Distributed Alarm Notification Systems based on IEEE 11073 SDC

To realize safety and interoperability issues using the service-oriented medical device connectivity standard family IEEE 11073 SDC, there are two basic ideas:

- An alarm producer defines two different alarm signals (one local and one remote) for one alarm condition.
- Remote alarm notifier (RANs) periodically announce their current state of remote alarm notification to the alarm producer.

Even if there is no local fallback signal physically or technically available, the approach is still possible. However, due to safety and liability issues, we recommend using a remote and a local fallback alarm signal. Thus, we describe the mechanism using both alarm signals in this paper.

A. Modelling Alarm Functionalities

The alarm producer models two different alarm signals being related to the same alarm condition. Both having the same manifestation (audible, visible, tangible) but one will be generated locally at the alarm producer and the other one will be generated remotely at a RAN. The local alarm signal is intended to be a fallback if there is no suitable network participant to generate the remote alarm signal or in case of failures, like crash of the remote device, connection loss, etc.

In IEEE 11073 SDC, all aspects of a service providing medical device are described semantically, including the relevant components for this work: alarm condition and both alarm signals. Elements are tagged with suitable term codes depending on the actual kind of alarms to be handled. A term code belongs to a coding system and ensures the semantical interpretability, e.g., MDC_EVT_ECG_TACHY (or 3120) from IEEE 11073-10101 nomenclature for Tachycardia.

Furthermore the alarm producer defines additional properties like priority, or generation delay for the alarm condition as well as manifestation, generation delay, and information whether the signal is latching or can be acknowledged, including acknowledge timeout for the alarm signals. On the one hand, this comprehensive description ensures the interpretability of the provided information for all participants of the networked medical device system, thus being able to notify the alarm. On the other hand, the alarm producer has the full control over the way the remote alarm notification has to be done, as the alarm producer defines all properties on its own. Thus, the first requirement is fulfilled.

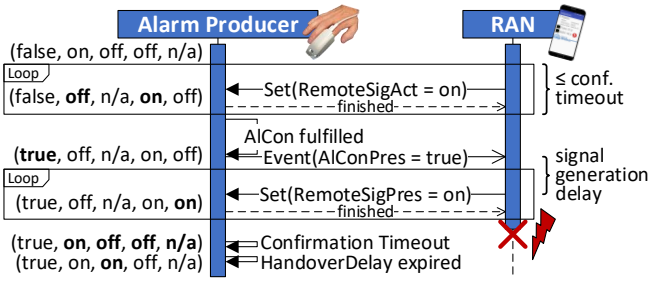

Fig. 1. Flow chart including system state of the alarm producer described in 5-tuple notation on the left. State changes highlighted with bold font. Abbreviations and 5-tuple as introduced in Sec. IV-B.1; conf. - confirmation.

B. Behavior at Run-Time

1) System Definition: To describe the behavior of the remote alarm notification system with local fallback alarm, five aspects have to be taken into account: The alarm condition presence and the remote alarm signal activation and presence

$$AlConPres \in \{true,\ false\}$$
$$RemoteSigAct \in \{on,\ off,\ paused\}$$
$$RemoteSigPres \in \{on,\ off,\ latched,\ acknowledged\}$$

as well as analogously the activation ($LocalSigAct$) and presence ($LocalSigPres$) of the local alarm signal, used as a fallback mechanism as described above. The activation state of the components is used to determine whether the component is currently operating or not. Please note, if an alarm signal is not operating (off or paused), the alarm signal presence shall not be interpreted. Thus, we highlight this by using "*n/a*" for not interpretable values.

Consequently, a 5-tuple can be used to describe the current state of the alarm producer *AP*:

$$AP = (AlConPres, LocalSigAct, LocalSigPres, RemoteSigAct, RemoteSigPres)$$

2) System Behavior in Regular Cases: As defined in Requirement 5 the remote alarm notifier (RAN) shall not be forced to implement service provider functionality to make its current alarm notification state available for the alarm producer. Hence, the alarm producer has to provide functionality to get this information. Therefore, the alarm producer offers a *set-alert-state* operation that allows the remote manipulation of relevant parameters of the remote alarm signal: Activation state, presence, and signal generation delay.

If a RAN intends and is ready to generate the remote alarm signal it sets the activation state to "*on*" and additionally sets the signal generation delay according to its capabilities. Now, the RAN is responsible to generate the notification in compliance with the alarm condition. The alarm producer will set the activation of the local alarm signal to "*off*", as it is no longer necessary to keep this alarm signal operating.

The effect of the invocation of the *set-alert-state* operation is limited to a time period defined and published in the device description of the alarm producer. Before this period has expired, the RAN has to retrigger the operation. This allows the alarm producer to determine any failure in the connection to the RAN within a defined time. This is illustrated in the upper part of Fig. 1 (first loop).

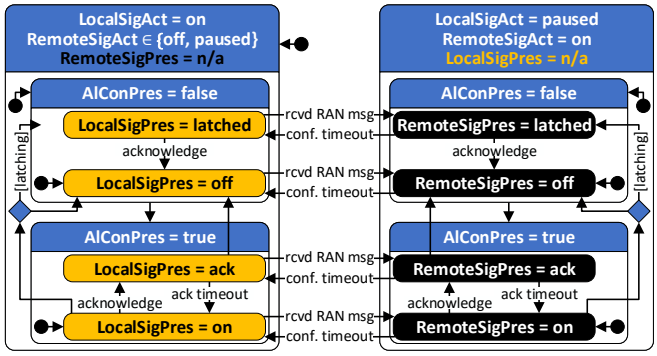

Fig. 2. State machine describing the relevant subset of states and transitions of the alarm producer. For abbreviations see Sec. IV-B.1; conf. - confirmation; rcvd - received; msg - message.

If the alarm producer detects the fulfillment of the alarm condition it will set *AlConPres = true*. This state change will be propagated by an event to any subscribed RAN. Within the signal generation delay, the RAN will generate the notification physically and will propagate its signal generation to the alarm producer by setting *RemoteSigPres = on*. According to the mechanism described above, the RAN sends a confirmation periodically. See middle part incl. second loop of Fig. 1.

As defined in the common alarm handling mechanisms of the IEEE 11073 SDC standard family, the remote alert signal can be acknowledged for a defined period. If the signal is defined as latchable, RAN will set *RemoteSigPres = latched* if the signal has not been acknowledged, but the alert condition is no longer present.

Fig. 2 shows the relevant subset of a state machine describing the states and state transitions of the alarm producer. The left part describes the state where the local alarm signal is operating. In the right part, the remote alarm signal is operating. Vertical transitions describe changes of the alarm signal presence according to the behavior of the alarm condition and possible acknowledgments. Horizontal transitions describe the change between operation of local and remote alarm signal. Transitions from left to right are caused by the availability of a remote alarm notifier (RAN). As described above, this is indicated to the alarm producer by receiving a corresponding message from the RAN. Transitions from the right to the left are cause by confirmation timeouts, as displayed in the lower part of Fig. 1.

Note, security aspects like encryption, authentication, and authorization are addressed by the MDPWS standard, using HTTPS and X.509 certificates, independent from our system.

3) Behavior in Exceptional Cases: To achieve Requirement 3, any remote error, like connection loss, unexpected high delays, crashes of RANs, etc. can be detected by the alarm producer due to the timeout mechanism and required periodical confirmation messages of the RAN as described above. If the timeout happens, the alarm producer will set the local alarm signal activation to "*on*" and the remote alarm signal activation to "*off*". From this moment, the alarm producer handles the alarm generation locally on its own, as it is no longer able to observe the behavior of the RAN.

As illustrated in the bottom part of Fig. 1, the alarm producer can delay the local alarm signal generation after the timeout. This delay allows a seamless handover from one RAN to another, without local signal generation. This reduces the noise at the alarm producer. The handover delay can be derived from the signal generation delay and invocation effect limit of the *set-alert-state* operation.

The RAN also reports the remote alarm signal presence periodically. Hence, the alarm producer is also able to monitor the correct alarm signal generation. If the RAN does not handle the signal presence correctly, the alarm producer can decide to stop the operation of the remote alarm signal, start the operation of the local alarm signal and therefore taking responsibility for alarm signal generation locally. This capability fulfills Requirement 4.

4) Ensembles with Multiple RANs and Alarm Producers: In a device ensemble with several RANs only one RAN will follow the mechanisms described above, acting as the "*responsible RAN*". This ensures that the alarm producer can be sure that at least one RAN generates the alarm signal in a way that fits to its risk management. All other RANs subscribe to the corresponding events of the alarm producer. Thus, these RANs receive all state changes including information about alarm condition, alarm signal, and also indirectly about the behavior of the "*responsible RAN*". On the one hand, this allows multiple RANs to generate the alarm signal possibly at multiple places and for multiple caregivers as well as a seamless handover from one "*responsible RAN*" to another. On the other hand, this reduces the workload for the alarm producer, as it has to monitor the behavior of only one RAN. As one has to act on the assumption that also very resource-constrained devices will use this mechanism, this is an important aspect.

Note, more powerful alarm producers are allowed to define several remote alarm signals for the same local alarm signal if this is reasonable for the use case and risk management. A possible use case would be an alarm producer that has to ensure that the alarm is generated at least by two different devices at different places. Therefore, the alarm producer could define two different remote alarm signals and define the additional requirement that the "*responsible RANs*" have to include their current location into the *set-alert-state* operation invocation messages using the mechanisms of the MDPWS safety context [8].

The handling of remote alarm signal acknowledgements sent by RANs that are not the "*responsible RAN*" depends on the risk management of the alarm producer. It is possible to reject these messages, if the alarm producer only trusts the monitored "*responsible RAN*", as well as to accept the acknowledgement from all RANs.

In a SOA all service providers act independently. Hence, a in device ensemble multiple different alarm producers are possible. Additionally, a network participant can act as RAN for different alarm producers, as there is no conceptual restriction or fixed assignment necessary. Consequently, Requirement 2 is fulfilled by the described mechanisms.

V. Demonstrator

For a proof of the presented concept, we implemented a small demonstrator. It contains two alarm producers: A

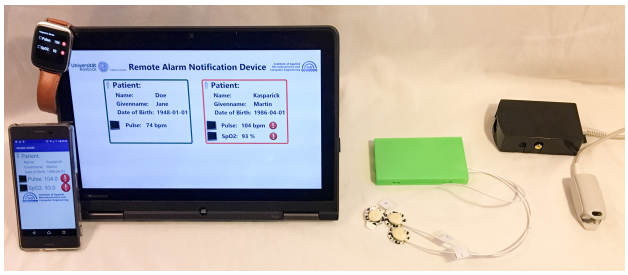

Fig. 3. Demonstrator (f.l.t.r.): Two remote alarm notifiers (RANs), smart phone incl. watch and PC application, and two alarm producers, ECG development board and pulse oximeter.

pulse oximeter providing the values and limit alerts for heart rate and oxygen saturation and a biomedical data acquisition development board providing value and limit alert for the measured heart rate, derived from an ECG waveform. For generating the remote alarm signals, we implemented two different remote alarm notifiers (RANs): A PC application representing a central ICU or OR dashboard and a smart phone application including a smart watch, representing mobile and wireless devices. As the smart watch application has no stand-alone functionality without the smart phone, they do not behave as two autonomous RANs. The smart watch acts as convenience extension of the smart phone. The smart phone's device logic has to care about connection loss between both devices. The demonstrator is shown in Fig. 3.

Both alarm producers provide audible and visible alarm notifications with remote and local fallback alarm signal. These alarm notifications demonstrate the whole mechanism for safe distributed alarm notifications. As both alarm producers have no capability for haptic feedback, an additional tangible alarm notification is provided without local fallback alarm signal. The implementation is based on different open source IEEE 11073 SDC communication libraries, OSCLib, openSDC, and SoftICE and on the DPWS library JMEDS.

The technical evaluation shows the suitability of the concept. The remote alarm notification allows a silent operation of the alarm producers. The safety mechanisms for faults can also be shown, like deactivation of the wireless connection, crash of RAN, etc. This small demonstrator allows for a technical evaluation with low complexity compared to today's and future device ensembles in ICU and OR and can be transferred to real-world scenarios. The underlying IEEE 11073 SDC technology has shown its suitability in [10] and in big and complex demonstrators at conhIT exhibitions 2015 to 2017 in Berlin, Germany, or within permanent demonstrators at the ICCAS of the University of Leipzig, Germany and at IMD of the University of Rostock, Germany. More than 30 different devices from more than 20 different manufacturers formed an interoperable networked medical device ensemble implemented in the cause of OR.NET project (www.ornet.org).

A clinical evaluation has to be done in the future. Until now, only a non-structured evaluation with six physicians (three anesthesiologists, two surgeons, and one internist) was performed. As all of them gave positive feedback, this can be seen as a hint for clinical relevance and suitability.

VI. Conclusion and Future Work

We presented a safe and distributed alarm notification system. It allows to generate alarm notifications at remote devices that are independent from the original alarm producing device, being not necessarily at the bedside. This includes the safe usage of mobile alarm notification devices, even connected via potentially unreliable, wireless connections. The system can thus reduce some of the basic problems of alarm fatigue and desensitization, as the alarms will be notified at the right place for the caregivers. The mechanisms are based on the new medical device interoperability standard family IEEE 11073 SDC, thus being manufacturer-independent.

As our distributed alarm notification system holds risk management and approval issues, it does not contradict the current "better-safe-than-sorry" mentality. While previous research on smart alarm systems did not enter the market and did not improve the problems in today's hospitals [2], [6], we therefore state that our mechanisms have a high potential to be implemented in PoC medical devices and to be used in the field. In contrast to the analysis of Konkani el al. [4], our distributed system has no single point of failure (SPOF). A real-world demonstrator has done the proof of concept. While limited and proprietary remote alarm notification systems are available on the market, interoperability and manufacturer-independence of a system holding safety requirements is highly innovative.

In the future, a deeper clinical evaluation should be done to investigate and improve the usability of the alarm management system based on the presented work. Furthermore, intelligent, computer-assisted alarm systems can be developed using our highly reliable alarm distribution mechanisms.

References

[1] M. Borowski, M. Görges, R. Fried, O. Such, C. Wrede, and M. Imhoff, "Medical device alarms," *Biomedizinische Technik/Biomedical Engineering*, vol. 56, no. 2, pp. 73–83, jan 2011.

[2] F. Schmid, M. S. Goepfert, and D. A. Reuter, "Patient monitoring alarms in the ICU and in the operating room," *Critical Care*, vol. 17, no. 2, p. 216, 2013.

[3] M. Cvach, "Monitor Alarm Fatigue : An Integrative Review," *Biomedical Instrumentation & Technology*, vol. 46, no. 4, pp. 268–277, 2012.

[4] A. Konkani, B. Oakley, and T. J. Bauld, "Reducing Hospital Noise: A Review of Medical Device Alarm Management," *Biomedical Instrumentation & Technology*, vol. 46, no. 6, pp. 478–487, nov 2012.

[5] D. Dyell, "Beyond Sound: Using Systems Integration to Advance Alarm Functionality," *Biomedical Instrumentation & Technology*, vol. 45, no. s1, pp. 72–75, mar 2011.

[6] T. Clark, "Closing the Clinical Alarm Gap," *24x7 Solutions for Healthcare Technology Management*, 2010. [Online]. Available: http://www.24x7mag.com/2010/09/closing-the-clinical-alarm-gap/

[7] N. A. Halpern, "Innovative Designs for the Smart ICU: Part 3: Advanced ICU Informatics," *Chest*, vol. 145, no. 4, pp. 903–912, 2014.

[8] M. Kasparick, S. Schlichting, F. Golatowski, and D. Timmermann, "Medical DPWS: New IEEE 11073 Standard for Safe and Interoperable Medical Device Communication," in *IEEE Conference on Standards for Communications and Networking (CSCN)*, Tokyo, Japan, oct 2015.

[9] ——, "New IEEE 11073 Standards for Interoperable, Networked Point-of-Care Medical Devices," in *37th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)*, Milan, Italy, aug 2015.

[10] M. Kasparick, B. Beichler, B. Konieczek, A. Besting, M. Rethfeldt, F. Golatowski, and D. Timmermann, "Measuring Latencies of IEEE 11073 Compliant Service-Oriented Medical Device Stacks," in *IECON - 43rd Conference of the IEEE Industrial Electronics Society*, oct 2017.