Tobias Pabst*, Dominik Stegemann, Christoph Georgi, Martin Kasparick, Julian Suleder, Thomas Neumuth, Max Rockstroh

TeleSDC

Concept for ISO/IEEE 11073 SDC in telemedicine across unreliable networks

Abstract: Telemedicine promises to increase the quality of emergency treatments. Besides the transfer of speech and video data, medical device and patient data will add additional value to the tele-guided emergency personnel. In this paper, we develop a concept for transmitting device and patient data via the open communication standards SDC in a telemedical context, including data transmission over mobile radio networks while considering the limitations of public networks, and opening new usage scenarios for telemedicine.

Keywords: 5G, Mobile Radio, Medical Device Interoperability, SDC, Emergency Care, Emergency Medical Service, IT Security, Telemedicine.

https://doi.org/10.1515/cdbme-2021-2102

1 Introduction

The standards family ISO/IEEE 11073 Service-oriented Device Connectivity (SDC) has been introduced to create interoperability between medical devices and to physically separate a device and its control. In essence, SDC standardizes communication between medical devices. There are data providers and data consumers. Data can include, among others, metrics, alarms, context information. Metrics describe the current state of a medical device, e.g., current settings or measured values. A standardized type as well as a standardized unit is assigned to each metric enabling a semantic interpretability independent of the concrete, vendor-dependent description of the metric. If specific metrics are out of predefined bounds or another unexpected condition occurs, an alarm informing all attached consumers can be issued. Context information is used to describe the patient, the location and other metainformation about the device and its context of use [1].

There are fields of medical emergencies in which a specialised physician is not available or, at least, not available in a short period of time. In densely populated cities, in nursing homes, in rural areas, in the mountains or on ships, physicians can support the treatment through upcoming telemedical applications [2]–[4]. SDC can transmit patient and device data to the physician to increase the quality of the telemedical support, thereby providing aid and support for diagnosis and decisions. In addition, information such as medication or pre-existing conditions can be obtained from the clinic to improve the patient's treatment. We call this 'TeleSDC'.

Multiple implementations of the SDC standards by different manufacturers exist. Current implementations require the devices to share the same local network. A connection over various foreign, unknown, and potentially unreliable networks must be established to allow for TeleSDC. This includes public landlines, mobile radios and satellite connections which is raising various quality, security, and management challenges. In this paper, we discuss those challenges and present possible solutions. This analysis is part of the ongoing MOMENTUM research project [5] which aims to interconnect ambulances and hospital's emergency command centres. Through this project, we connected with various physicians and medical device manufacturers to strengthen our analysis. However, we can only examine selected significant aspects in detail in the scope of this paper.

2 Methods

In this section, we discuss the methods and the before mentioned challenges. We assume that the setup contains two local networks. At least one of these networks is not connected via landline but via mobile radio or satellite. That network will be called the *emergency network* and it is located at an emergency site. The other one will be called the *clinical network,* and this is where the tele-physician operates. Both

***Corresponding author: Tobias Pabst:** ICCAS[1]
Dominik Stegemann, SurgiTAIX AG, Herzogenrath**,** Germany, **Christoph Georgi**, ICCAS [1], **Martin Kasparick**, Institute of Applied Microelectronics and Computer Engineering (University Rostock), Rostock, Germany **Julian Suleder**, ERNW Research GmbH, Heidelberg, Germany, **Thomas Neumuth**, ICCAS [1], **Max Rockstroh**, ICCAS[1]
[1] (Innovation Center Computer Assisted Surgery), (Institute of Faculty of Medicine, University Leipzig), Leipzig, Germany, Firstname.Lastname@medizin.uni-leipzig.de

networks contain multiple SDC providers and SDC consumers that should communicate with each other.

2.1 Management Challenges

First of all, a **shared IP range** is necessary to achieve SDC communication. Exposing the local networks or the medical devices to the Internet can solve this by addressing every device by its public IP address. However, this solution raises disadvantages, as not every network can provide public IP addresses and their usage would present an additional attack vector. A virtual private network (VPN) overcomes those issues. By installing VPN gateways in the networks and assigning a virtual IP address to every device, device-to-device communication can be tunnelled through the VPN gateways over a VPN host, thereby avoiding that the medical devices are exposed directly to the Internet. Furthermore, the VPN solution simplifies usage, as devices do not need to be modified if VPN gateways are set as standard gateways.

Second, SDC devices need proof of authenticity to communicate, which means they need a **shared trust anchor** realized over TLS client certificates. It cannot be reasonably assumed that all devices share the same common trust anchor across all networks and changing certificates during runtime is undesirable. We propose to create a particular SDC component with two independent trust anchors, called *SDC gateway*, to cope with these challenges.

By placing one **SDC gateway** in each local network, the medical devices do not need to adjust their certificates. They will only communicate with their local SDC gateway and never directly with a device in the other network. The SDC gateway shares one trust anchor with the devices in its local network and one with the SDC gateway on the other side of the VPN. As a result, only the SDC gateways need to use the VPN.

2.2 Security Challenges

Exposing devices to the Internet will add **threat levels** compared to operating in an only local SDC network. Important security goals are confidentiality, integrity, and availability of a communication system. The designed VPN provides layers of security for the system by encrypting the communication and restricting access to that network to only authenticated and authorized parties, therefore ensuring confidentiality and integrity of the network. In order to use the advantages of a VPN, it is essential for providers of TeleSDC to make sure that the VPN is hosted in a trustworthy manner and that there is a trustworthy and independent agency that manages VPN login data, VPN addresses and VPN participants.

To guarantee the **availability** of the VPN connection, redundant components of the system are recommended. However, even small connection losses could lead to sensitive medical situations. SDC devices already account for connection losses in their risk management. Additionally, the risk management of SDC devices needs to be extended to cover network-related issues to allow for telemedicine usage.

2.3 Quality Challenges

The solution offered prior provides a functional TeleSDC network. However, communicating over unreliable networks further highlights vulnerabilities such as a higher chance of connection loss, changing IP addresses during runtime, uncertain and variable bandwidth (due to unknown networks and moving devices) and higher latency.

With the usage of an SDC gateway, only one component will need to reconnect after a connection loss, reducing the lost time. In addition, the VPN handles **IP address changes** automatically and transparently for the devices and users.

If the Internet connection is slower than needed, a **bandwidth shortage** occurs. In this event, the SDC gateway could decide which data should be prioritized based on the importance of the devices. For example, a tele-physician could request an endoscope image stream and device control via SDC. If dropping other data streams, e.g., the audio connection to the local paramedic, would ensure a stable dataflow for the endoscope, it should be done to guarantee the best treatment.

Compared to a local network, there will always be higher **latency**. Therefore, the SDC gateway could be extended to measure current delay and jitter. Similar to the bandwidth shortage behaviour, the gateway could then display warnings or disable data transfers. However, future developers of TeleSDC systems need to make sure that their systems do not add too much further delay to the connection, and there should be detailed plans for cases of poor connection quality.

The usage of an SDC gateway provides further advantages.

2.4 Advantage 1: Risk Management for Telemedicine

The SDC gateway would be one component in the emergency network that encapsulates all SDC devices from the clinical network. Thus, all actions and requests originating from the SDC gateway can be identified as emanating from the remote side. Therefore, devices at the emergency site can distinguish requests from the emergency physician and the tele-physician and take that into account for their risk management, providing specialization for the new usage scenarios.

2.5 Advantage 2: Local buffering

With a central component to handle incoming and outgoing SDC traffic, it is possible to implement buffering. A buffer on the clinical side would have the advantage that no data needs to be sent twice. Buffering in the emergency network can collect data (e.g., heart rate) and send it in bulk to allow for a faster data analysis by the tele-physician. This will occur after a connection loss as well as at the beginning of a telemedical session.

3 Results

The considerations in the previous chapter suggest the usage of an SDC gateway and a system was designed that meets the stated requirements. To prove its feasibility, a demonstrator was implemented and tested. In this chapter, we explain its design and implementation details.

3.1 Concept

The SDC gateway concept consists of two components. The first component in the emergency network is called *gateway provider* and the second component in the clinical network is called *gateway consumer*. They are designed differently, as the gateway provider can provide additional services, e.g., controlling the connection in case of bandwidth shortage. Each of the two components resides partly in the local network and the VPN which is used for communication between the two components. In this concept, every operation, state, and device data are transmitted according to ISO/IEEE 11073 SDC standards.

Figure 1 shows the initialization phase. First, a *mapping component* of the gateway provider discovers all available *MDS* (medical device systems) and aggregates them into one single internal MDIB (Medical Data Information Base) with multiple MDS, we call *internal aggregation*. For this, a suitable mapping strategy is needed. The mapping component subscribes to all metrics, contexts, and alarms of all found devices and forwards everything through the mapping to their counterparts in the internal aggregation.

The gateway consumer will subscribe to the gateway provider's internal aggregation via the VPN connection, cloning its content and creating an *emergency network twin*. The twin will act as a single device in the clinical network, representing the whole emergency network while still providing a single, manageable connection through the VPN. The internal aggregation and the emergency network twin are simultaneously SDC provider and SDC consumer. Still, only the SDC consumer of the gateway consumer and the SDC provider of the gateway provider reside in the VPN.

After the initialization is complete, local devices in the emergency network can establish SDC communication with the emergency network twin. This includes reading and subscribing to changes of metrics and changing settable metrics, performing predefined operations, and accessing contexts and alarms of the devices.

To allow backpropagation to the emergency network, any changes made by local SDC devices to the emergency network twin must be relayed by the twin through the VPN as well as by the internal aggregation through the mapping to the correct device in the emergency network.

The mentioned mapping component needs a good mapping strategy to avoid conflicts in the aggregated MDIB. Strategies include a hardcoded strategy, a type-based strategy revolving around the IEEE 11073-10101 nomenclature, or a user-defined mapping, e.g., using a graphical user interface.

Figure 2 shows the procedure if a metric is set in the clinical network. First, a local device initiates a set request (1) to the emergency network twin that will be forwarded over the VPN (2) to the internal aggregation. It will again be forwarded (3) through the mapping to the device, where the metric originated from. There, it will cause a change of state, which in turn causes an update event for the changed metric. The change report and the new value will be reported back to the mapping component, where it will be forwarded to the internal

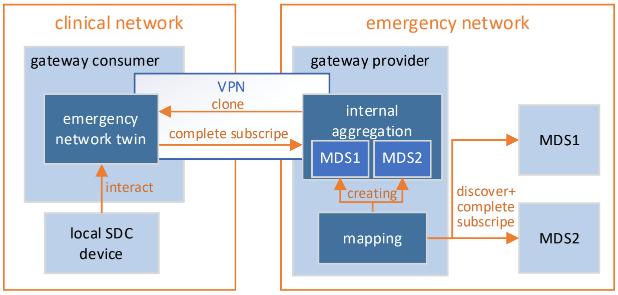

Figure 1: Initial construction of gateways

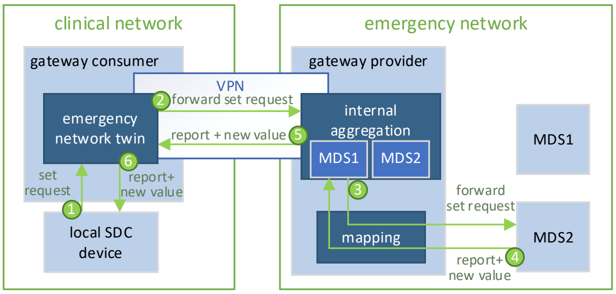

Figure 2: Data manipulation from clinical network

aggregation (4), then to the emergency network twin (5) and finally to the SDC device, where the set request originated from (6).

In the case, an SDC device at the emergency network generates a new value with no external trigger, the value update will follow the path (4,5,6) equivalent to the reporting process because of the subscriptions of the mapping component, the internal aggregation, and the emergency network twin,

3.2 Implementation and Test

A demonstrator application was written in C++ using the open-source library SDCLib/C [6], [7] of SurgiTAIX AG to show that the concept is feasible and correctly transfers data between two networks. Furthermore, the demonstrator implemented the base functionalities of aggregating metrics and of sharing the metrics into a different network.

A type-based mapping strategy was introduced for the internal aggregation. This strategy uses the nomenclature terms defined in ISO/IEEE 11073-10101 which must be set on each metric. Those nomenclature terms provide semantic information about the content of a metric by assigning them a unique number which encodes the metric's function. For example, each pulse oximeter will encode its SpO2 measurement with the code 150456, independent of the vendor. However, this mapping strategy is only sufficient for this testing purpose, as it could not handle two metrics of the same code.

The application was tested using Ilara GmbH's OR.NET VPN, a VPN explicitly used for testing SDC devices. In addition, a pulse oximeter was used as a testing device. In the test, the states of the pulse oximeter, the emergency network twin, and the internal aggregation were monitored. The test was deemed successful because the states of all three devices showed the same behaviour, although exposing a minimal delay.

4 Conclusion

This paper presented the needs, requirements, and advantages for interconnected SDC networks (TeleSDCs). A general concept was elaborated based on those requirements. This concept allows connecting two networks to provide SDC communication between them and control the connection in an arbitrary manner. A demonstrator software was implemented to prove the validity of the concept. The software showed that inter-network SDC communication is possible. However, with further development of the SDC standard and additional development of the risk management and the approval strategies of medical device manufacturers, this concept also needs to be adapted in the future.

In the MOMENTUM research project, a system for networking ambulances, hospitals and telemedicine providers based on 5G mobile radio is currently being developed. In this context, TeleSDC represents an integral component for providing emergency care based on telemedical technologies and services. Lastly, the application is not limited to ambulances, but, in the future, may also support care in rural areas and hard-to-reach places such as ships and even space stations.

Author Statement

Research funding: This work is partially funded by the German Federal Ministry of Education and Research (BMBF) with grant number 16KIS1030.
Conflict of interest: Authors state no conflict of interest.
Ethical approval: The conducted research is not related to either human or animal use.

References

[1] M. Kasparick et al., “OR.NET: a service-oriented architecture for safe and dynamic medical device interoperability,” Biomed. Tech. (Berl), vol. 63, no. 1, pp. 11–30, Feb. 2018, doi: 10.1515/bmt-2017-0020.

[2] N. van den Berg, H.-J. Grabe, H. J. Freyberger, and W. Hoffmann, “A telephone- and text-message based telemedical care concept for patients with mental health disorders - study protocol for a randomized, controlled study design,” BMC Psychiatry, vol. 11, no. 1, p. 30, Feb. 2011, doi: 10.1186/1471-244X-11-30.

[3] Dr. M. Skorning et al., “„E-Health“ in der Notfallmedizin – das Forschungsprojekt Med-on-@ix,” springermedizin.de, no. 3/2009, Mar. 2009, Accessed: Jun. 30, 2021. [Online]. Available: https://www.springermedizin.de/e-health-in-der-notfallmedizin-das-forschungsprojekt-med-on-ix/8003998

[4] C. Metelmann et al., “Prähospitale Telenotfallmedizin,” Notfallmedizin Up2date, vol. 15, no. 4, pp. 381–395, Dec. 2020, doi: 10.1055/a-1131-6472.

[5] M. Rockstroh et al., “Towards an integrated emergency medical care using 5G networks,” Curr. Dir. Biomed. Eng., vol. 6, no. 3, pp. 5–8, Sep. 2020, doi: 10.1515/cdbme-2020-3002.

[6] A. Besting, S. Bürger, M. Kasparick, B. Strathen, and F. Portheine, “Software design and implementation concepts for an interoperable medical communication framework,” Biomed. Tech. (Berl), vol. 63, no. 1, pp. 49–56, Feb. 2018, doi: 10.1515/bmt-2017-0012.

[7] surgitaix, surgitaix/sdclib. 2021. Accessed: Jul. 06, 2021. [Online]. Available: https://github.com/surgitaix/sdclib