Open Software Platform
for Cyber-Physical Medical Systems

Jörg-Uwe Meyer
MT2IT Research
MT2IT GmbH & Co. KG
Ratzeburg, Germany
joerg-uwe.meyer@mt2it.com

Abstract: Fail-safe open software platforms for cyber-physical medical systems (CPMS) are expected to securely host medical applications of medical devices, clinical systems and health repositories for the purpose of safe healthcare delivery to patients at the point of care. Secure and reliable ad-hoc connections to medical systems and health records are mandatory when health professionals need immediate access to the patient's live vital data and electronic medical records during individual medical procedures. Here, we report about a service-oriented open software platform that has been developed for cyber-physical networks of distributed medical systems. An automated data logging cyber-physical software system for medical procedures is described, which is characterized by secure user authorization, standardized device and system communication and software-assisted guidance utilizing a WHO surgical safety checklist.

1 Introduction

Cyber Physical Systems (CPS) are defined as systems of collaborating computational elements controlling physical entities [1]. Health related applications of CPS include high confidence medical devices and systems, assisted living, and telemedical applications [1]. Cyber-physical medical systems (CPMS) are described as communicating networks of regulated medical systems which can be accessed through the Web. The CPMS might resemble the characteristics of an medical IT network, which is defined as a general purpose information technology (IT) network in which at least one medical device is incorporated and which is commonly connected to a clinical information system [2]. A medical IT network is considered a point-of-care (PoC) medical device and system network when healthcare is delivered live to the patients. This paper describes an open software platform for a cyber-physical medical device data system in surgery. An automated data logging software of connected medical

---

systems is proposed which includes a surgical checklist application for enhancing patient safety and objective documentation.

2 Service-Oriented Medical Platform

2.1 Vendor-neutral Interoperability Gateway

The central component of the service oriented medical platform is a vendor-neutral interoperability gateway which hosts the middleware and orchestrates applications which derive from medical systems in the point-of-care (PoC) network communicating with disparate health-IT networks. A schematic of the interoperability gateway connecting medical devices and systems in the IT and PoC network is illustrated in Fig. 1.
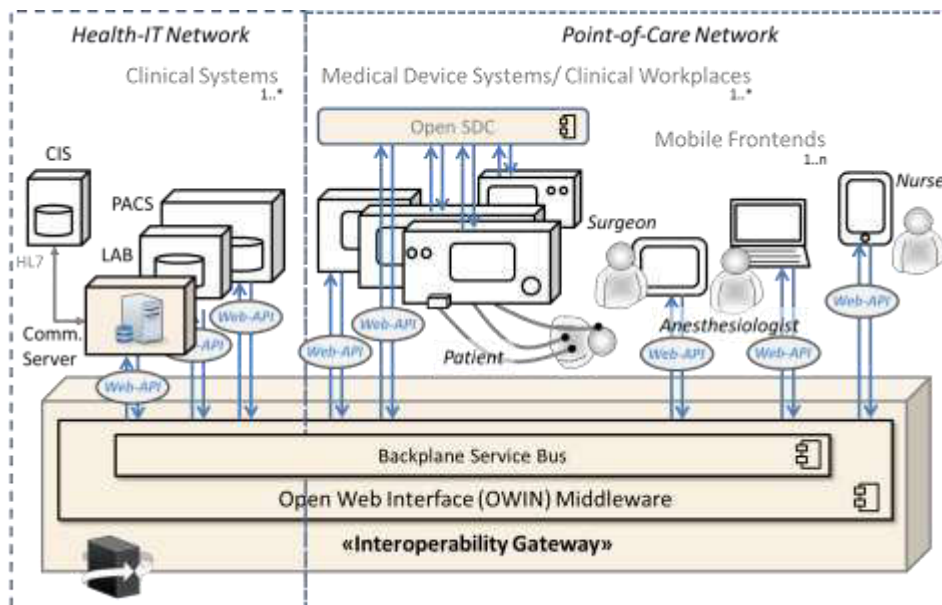

Figure 1: Schematic of an interoperability gateway which integrates systems and applications in the health-IT and point-of-care networks.

Individual or Open SDC[2] networked medical devices are connected to the Open Web Interface (OWIN)[3] middleware of the gateway through Web application programming interfaces (Web-APIs) between Web server and the Web client applications. User agents are Web client applications of browser programs, commonly found in frontend devices. A standard has been proposed regarding the architecture for distributed systems of medical devices in high acuity

---

[2] Open SDC: http://sourceforge.net/projects/opensdc/
[3] Open Web Interface (OWIN): http://owin.org/

environments [3]. The openSDC effort has led to standardization documents which are proposed by the IEEE EMBS 11073 & HL7 Health Care Devices (DEV) Working Group [4].

The user-specific surgical man-machine interfaces for the surgeons, anesthesiologists and nurses employ the same connectivity paradigm as described above. The medical frontends provide user access through a user-specific interactive browser interface. The frontend interface acts as a client user-agent connected to the gateway through a Web-API. The Web-API interfaces applications in both, the HTTP-based gateway Web server and the Web browser of the frontend client. The API is designed as a RESTful[4] interface to a defined request-response message system, expressed in JSON[5].

The Web-API can optionally be designed as a FHIR[6] interface between resources as JSON representations. The Fast Healthcare Interoperability Resources (FHIR) implementations define a set of resources that represent granular clinical concepts[7]. Each of the resources has a predictable URL. The resources can be managed in isolation or bundled into complex documents. If suitable, open internet standards are used for FHIR data representation.

2.2 Secure User Access to the Open HealthWeb Platform

The open service-oriented health software platform and its capability to implement clinical workflow-based health services have been described elsewhere [5]. Here, we illustrate individual user registration for securely accessing authorized patient information. The system provides patient data to the individual user according to the identified role and individually granted user authorization. The Web-API of the local login scenario uses the standardized OAuth2 mechanism to authenticate the request and to manage data flow according to authorization credentials. A simple scheme of the login credential flow is depicted in Fig. 2. The OAuth2 credential flows are managed by the gateway's OWIN middleware. The OWIN defines a standard interface between .NET Web servers and the implemented Web applications.

In this scenario, Web-API controllers act as resource servers. An authentication filter validates access tokens. When a controller or action has an "Authorize" attribute, all requests to that controller must be authenticated. Otherwise, authorization is denied, and the Web-API returns an error for unauthorized access[8]

---

[4] RESTful Interface: http://en.wikipedia.org/wiki/Representational_state_transfer
[5] JSON: http://en.wikipedia.org/wiki/JSON
[6] FHIR-API: http://www.hl7.org/implement/standards/fhir/http.html
[7] FHIR: http://wiki.hl7.org/index.php?title=FHIR
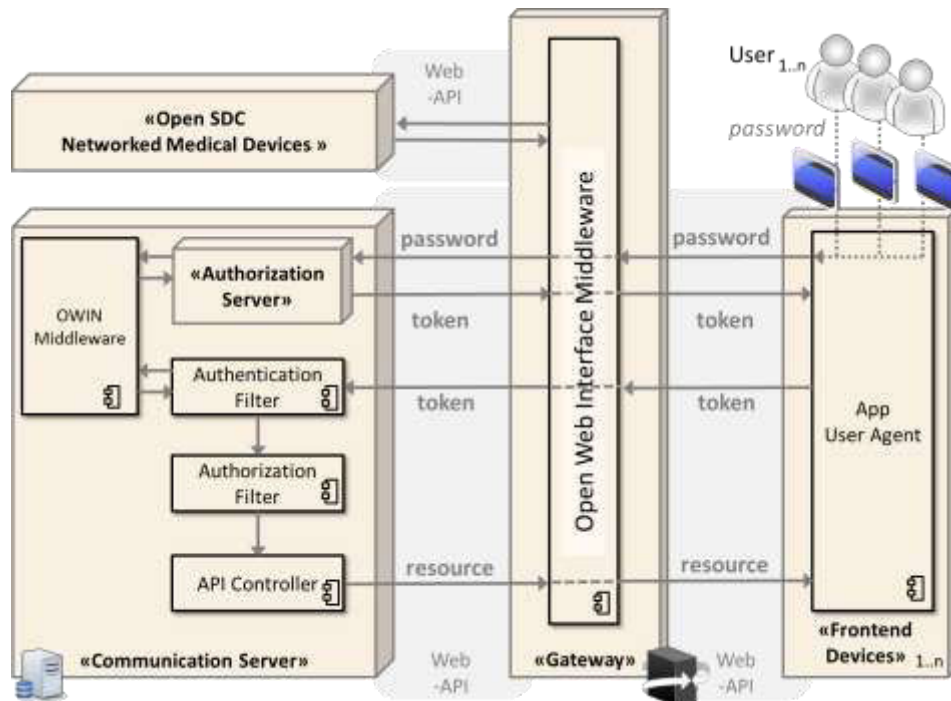[8] OAuth2 API Controller: http://www.asp.net/web-api/overview/security/individual-accounts-in-web-api

Figure 2: Illustration of the fail-safe OAuth2 login procedure of multiple users (e.g. doctors, nurses, caretakers) requesting access to resources in the cyber-physical IT network which hold patient data. The depicted platform is composed of 1) user frontends and the Open SDC network of medical devices at the point of care 2) the gateway for managing the Web-APIs between the systems and orchestrating the data flow and 3) the communication server with authentication and authorization components responsible for securely accessing patient data. The OAuth2 standard is employed which is particularly suited to provide user-specific authorization flows for web applications[9].

Automated Surgical Safety Checklist

An automated data logging system is built in software, which automatically records user interactions, events and alerts from data communication between the devices and systems. The software includes a graphic user interface that is specifically designed to assist the OR safety manager of maintaining live a surgical safety checklist (SSC) as promoted by the World Health Organization (WHO). The WHO SSC was developed after extensive consultation with health professionals aiming to decrease errors and adverse events, and to increase teamwork and communication in surgery . The checklist is designed to guide communication among the health professionals and with the patient

---

[9] OAuth2 http://oauth.net/2/

aimed to enhance patient safety in surgery. Implementation of SSC in surgical routines has proven to significantly reduce morbidity and mortality in surgery. The WHO SSC application is implemented in software as a request/response routine with the OWIN middleware as a standard interface between the gateway server and the SSC application.
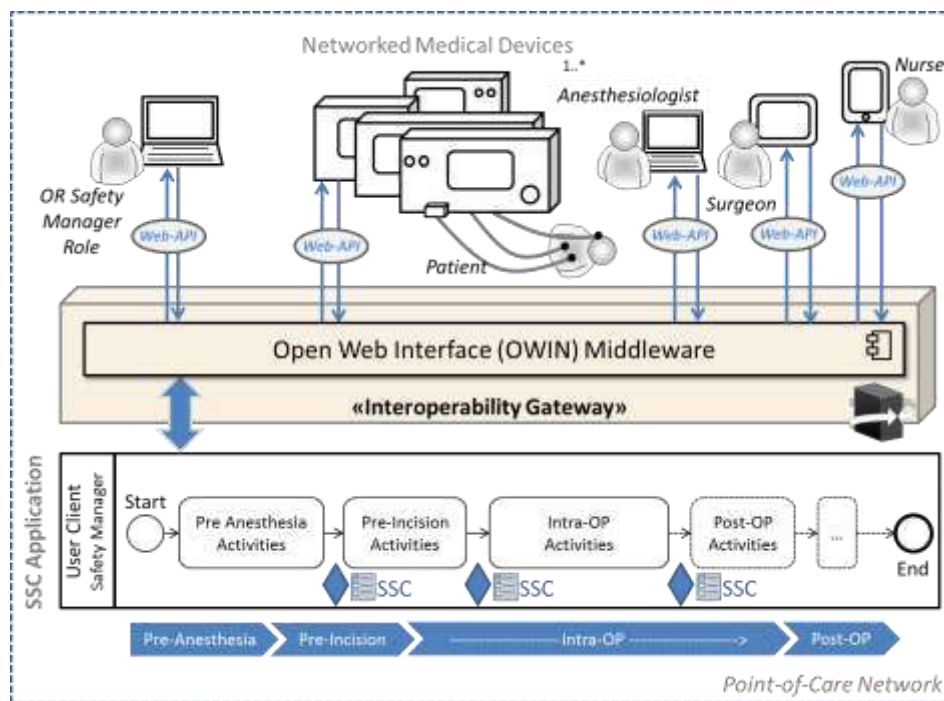

Figure 3: Integration of the WHO Surgical Safety Checklist (SSC) as a software module in the Open Web Interoperability (OWIN) middleware of the Interoperability Gateway. The OWIN middleware provides cross domain request/reponse functionalities of the SSC module between the frontend user agents and the gateway server. The software supports the role of an OR safety manager guiding and documenting communication with the patient before induction of anesthesia and among the surgical team before skin incision and until the end of the intraoperable procedure.

Discussion and Perspectives

Our work concerns the development of a fail-safe open software platform for cyber-physical medical systems in surgery. This paper has described a concept and technical implementations of users securely accessing the medical IT network during live surgical procedures. The OAuth2 standard is employed which is particularly suited for healthcare

delivery organizations (HDOs) to grant user specific authorization flows when accessing medical device and Health IT system networks. The deployment of a Health IT communication server and a vendor-neutral interoperability gateway has proven to be a feasible infrastructure for the open software platform. Multiple Web-APIs to medical device networks and health IT systems are managed through implementing an established standardized open web interface middleware as a request and response pipeline across device and systems domains.

The WHO Surgical Safety Checklist application is presently built as a demonstrator for automated device, system and workflow integration in the surgical room.

The SSC application under development is a project in the framework of the German federally funded flagship project "OR.NET", in which more than 50 partners from industry and research participate [6]. OR.NET objectives include the development of a service-oriented medical platform which promotes fail-safe and secure interoperable interactions of medical device networks in the operation room (OR). The DKE standard working group 1000.8.3 has been established that contributes to the Open SDC standardization process and endorses the proposed HL7 IEEE standards p11073-10207, p11073-20701 and p11073-20702.

Future works concerns the development of software routines for testing the health Web platforms in clinical environments and for verifying routines for compliance with ISO and IEC standards and with profiles of the "Integrating the Healthcare Enterprise (IHE) association including FHIR.

Acknowledgment

References

[1] E. A. Lee, "Cyper Physical Systems: Design Challenges", http://www.eecs.berkeley.edu/Pubs/TechRpts/2008/EECS-2008-8.html, EECS Department, University of California, Berkeley, January 23, 2008.

[2] M. Janssen and R. Schrenker, "Guidelines From 80001 Maintaining a Medical IT Network", in Biomedical Instrumentation & Technology, July/Aug 2011, pp. 295-299.

[3] S. Schlichting and S. Pöhlsen, "An architecture for distributed systems of medical devices in high acuity environments - A Proposal for Standards Adoption"; http://www.hl7.org/documentcenter/public_temp_C17326F5-1C23-BA17-0C77F7AEBDCABB5C/wg/healthcaredevices/20140121%20An%20architecture%20for%20distributed%20systems%20of%20medical%20devices%20in%20high-acuity%20environments.pdf

[4] S. Schlichting, "openSDC Update", Joint meeting of IEEE EMBS 11073 & HL7 Health Care Devices (DEV) WG, San Antonio, 2015/01/20. http://www.hl7.org/Special/committees/healthcaredevices/docs.cfm

[5] J.-U. Meyer, "Open SOA Health Web Platform for Mobile Medical Apps, 8th IEEE International Workshop on Service-Oriented Cyber-Physical Systemsin Converging Networked Environments (SOCNE) in conjunction with ETFA 2014, Barcelona, Spain, September 16st, 2014

[6] OR.NET Flagship Project, http://www.ornet.org/?lang=en, Kick-off meeting, October 2, 2012, Heidelberg, Germany.

[7] Integrating the Healthcare Enterprise (IHE), www.ihe.net , retrieved on 2014-06-13.