International Workshop on safety & security of (wireless) medical sensor networks

TU Delft - 21 January 2014

Organisers:
The Security and Medical Devices subgroups of the European Workshop on Industrial Computer system (EWICS) in cooperation with TU Delft (Safety & Security Science Group), TU Delft Safety & Security Institute, and the Delft Health Initiative.

Scope of the workshop
The workshop addresses the complex issue of networked (wireless) systems in which medical sensor devices are configured for applications that are critical for patients. With the first edition of the IEC 80001, it is recognised that network infrastructure and content flows need to be considered together in order to assess system vulnerability, availability and integrity. However, there is still a long way to go to ensure that networked medical systems are robust and trustworthy when they are operational. Examples of Electronic Patient File (EPF) network breakdowns in the UK and the USA show that dependability still starts in design details of the system components. The vulnerability increases with the complexity of the network configuration and its environment.

This workshop will focus on wireless sensor networks because this is a rapidly emerging application domain where:
- the trend is to send patients home earlier rather than keeping them in a hospital,
- there is an increased security awareness, there are also increasing attempts to gain unauthorised access to medical systems, and
- public networks could be supporting safety-critical applications.

Sensors may also be activators, but even for monitoring sensors timely and correct readings are of paramount importance.

Wireless medical sensor systems may extend into the patient's home and within the community, and these may pose additional challenges where:
- There are multiple interacting applications from different suppliers
- Data is transferred across a number of different types of networks including the internet

- There are diverse environments with little operational control (e.g. patient's home)
- The system control may be distributed over several sites involving large distances
- There may not be a single organisation responsible for the provision of the system
- The patient as user cannot be assumed to be adequately trained and be familiar with safety and security requirements.

Who should attend?

This workshop is intended to provide an active forum to participants from clinical users, industry, network service providers, researchers, standardisation bodies and regulators to discuss emerging issues of safety, security and risk management related to medical sensor devices in network configurations that are not yet adequately addressed in standards, other regulation or guidelines.

Workshop Aims:

1. To explore safety and security threats of networked medical devices;
2. To assess the extent to which relevant standards are applicable and to identify the gaps that exist in the standards (e.g. 80001);
3. To identify gaps in the current research and to determine possible future research areas;
4. To foster collaboration and exchange of ideas through a community of practice beyond the workshop.

Workshop structure

In the morning, the workshop is organised into sessions that include short presentations by leading experts from the medical profession, medical sensor manufacturers, standards and security domains as well as end users that are intended to raise issues and to stimulate discussion. In the afternoon, group discussions on key issues from the morning's presentations will be held in breakout sessions followed by a plenary to discuss the conclusions drawn during the breakout sessions. A panel session will discuss issues raised during the day and to conclude the workshop, the moderator will give a brief summing up.

Delegates are welcome to attend the EWICS TC7 meeting on the following morning, where the issues raised during the workshop will be further discussed and future work including the case study will be progressed. For further information on EWICS TC7, please see www.ewics.org.

Workshop Programme

8:30 Registration + coffee

9:00 Welcome and Introduction to the workshop

9:10 Setting the Scene - EWICS Case Study: **Odd Nordland** [SINTEF, Norway]

9:45 Networks Standards Session: **Oliver Christ** [PROSYSTEM AG, Germany]

10:15 Medical Sensor Developer Session: **Geoff Duke** [Johnson & Johnson, UK]

10:45 - 11:00	**Coffee Break**

11:00 Network Security Session: **Karin Bernsmed** [SINTEF, Norway]

11:30 Medical Network Vulnerability Session: **Reinout Hensbroek** [TNO, The Netherlands]

12:00 Medical Profession Session: **Martin Janssen** [UMC St. Radboud, The Netherlands]

12:30 - 13:15	**Lunch**

Afternoon

13:15 Breakout sessions

14:45 Reporting back from breakout sessions

15:45 - 16:15	**Coffee Break**

16:15 PANEL SESSION

17:00 Summing-up by moderator

17:15 Closure and informal get-together

Registration

Attendance to the workshop is limited and the organisers seek a spread of delegates from different countries and over the different sectors of health care, industry, regulation & standardisation, research and end users. To achieve these aims, attendance at the workshop will be by invitation. The workshop fee is 75€ to cover catering and organisational expenses.

Those wishing to attend the workshop are requested to send an email message ASAP with the following information: name, affiliation, sector, email address to Erika van Verseveld:

f.g.vanverseveld@tudelft.nl.

Delegates invited to the workshop will be sent further workshop information, including travel to the venue, and an invoice of 75€ for the workshop fee to be paid within 15 days. Upon receipt of the payment, a confirmation of registration will be sent. If payment is not received in time, the place may be given to another person.

At the end of the workshop, delegates will receive a certificate of participation.

For further inquiry, contact Floor Koornneef, Safety & Security Science Group, email: f.koornneef@tudelft.nl, phone: +31 15 2786437

Venue: TU Delft, t.b.a.

TU Delft