FDANEWS PRESENTS THE

Space Is Limited, Register Today!

SOFTWARE AND CYBERSECURITY RISK MANAGEMENT FOR MEDICAL DEVICES

UNDERSTANDING THE FDA'S POSITION AND BEST PRACTICES FOR COMPLIANCE

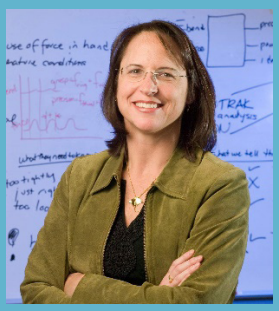
AN INTERACTIVE WORKSHOP PRESENTED BY FDANEWS AND GESSNET

OCT. 14-15, 2015

HILTON WASHINGTON DC/ROCKVILLE HOTEL & EXECUTIVE MEETING CENTER • ROCKVILLE, MD

YOUR INSTRUCTORS

FUBIN WU
Workshop Leader and Co-Founder of GessNet — software and consulting company specializing in medical device risk management



LISA SIMONE, PH. D.,
Software Review Team Lead and Policy Advisor, Office of Blood Research and Review, CBER, FDA

This workshop — **chaired by internationally renowned expert Fubin Wu** — has been specifically designed to provide you with industry best practices to achieve compliance and effectively assure medical device software safety.

In fact, it's a once-in-a-lifetime opportunity **to learn how the FDA expects you to manage the risks of your medical devices that contain software.**

In two days of intensive sessions, you will be brought up to date on the FDA's latest research on medical device software best practices, software risk management related standards and guidances and key success factors for effective software risk management.

Plus, in a special bonus, you'll find out more about assurance levels — and what it will take to convince regulators — in one of **four class exercises**, always a popular and valuable way to learn. Our four class exercises cover:

1) risk analysis for medical device mobile apps

2) risk assessments and risk controls for software hazards

3) cybersecurity risk analysis

4) cybersecurity risk assessments and risk controls

Spread throughout the course will be lessons in applying these key software risk management related standards and guidances to your software development processes:

- ISO 14971:2007 and EN ISO 14971:2012, IEC 62304 Medical Device Life Cycle Process, IEC TR 80002-1 Application of ISO 14971 for Software
- FDA Guidance on Mobile Medical Applications, Cybersecurity in Medical Devices, Infusion Pump Total Product Life Cycle

During each teaching session, Mr. Wu and Dr. Simone will share techniques and best practices on how to:

- Identify software related risks
- Identify software risk control and mitigation measures
- Assess and evaluate risk contributed/caused by software (premarket and post-market field issues)
- Assure the completeness and adequacy of risk management
- Communicate risk management information throughout the life of the product
- Key success factors for effective software risk management

Here's what you can expect to walk away with at the end of two intense days at **Software and Cybersecurity Risk Management for Medical Devices:**

- Understanding of how medical device manufacturers can overcome both technical and regulatory compliance challenges
- The resources and tools to help you succeed
- The medical device industry's best practices
- The FDA's latest updates on medical device software best practices

Special Take-Home Resource Kit:

You'll take home a jam-packed resource kit with **more than 20 templates, checklists, case studies, guidances and supporting information.** These are the tools that will help you effectively carry out the lessons you've learned over the two-day conference.

DAY ONE

8:00 a.m. – 8:30 a.m. | **REGISTRATION AND CONTINENTAL BREAKFAST**

8:30 A.M. – 9:00 A.M. | **WELCOME AND INTRODUCTIONS**

9:00 a.m. – 10:00 a.m.

I. Software Characteristics Comparing to Hardware

a. Understanding the difference between software and hardware
b. Understanding software quality and reliability engineering
c. Challenges of software risk management and cybersecurity

II. FDA's Analysis of Software Recalls

a. What kinds of software issues causing recalls
b. What kinds of devices have more software issues
c. What are the common types of causes for software calls

10:00 a.m. – 10:15a.m. | **REFRESHMENT BREAK**

10:15 a.m. – 11:00 a.m.

III. Overview of FDA Software & Cybersecurity Related Guidance

a. Mobile Medical Applications (Feb 2015)
b. Medical Devices Data Systems, Medical Image Storage Devices and Medical Image Communications Devices (Feb 2015)
c. Total Product Life Cycle: Infusion Pump (Dec 2014)
d. Content of Premarket Submissions for Management of Cybersecurity in Medical Devices (Oct 2014)
e. FDASIA Health IT Report – Proposed Strategy and Recommendations (April 2014)
f. NIST Framework for Improving Critical Infrastructure Cybersecurity (January 2014)
g. Radio Frequency Wireless Technology in Medical Devices (Aug 2013)
h. General Principles of Software Validation
i. Content of Premarket Submissions for Software Contained in Medical Devices
j. Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software

11:00 p.m. – 12:15 p.m.

IV. Overview of Software & Cybersecurity Related Standards

a. ISO 14971:2007, EN ISO 14971:2012,
b. IEC TR 80002-1 Application of ISO 14971 for Software
c. IEC 62304 Medical Device Software Life Cycle Process, IEC 82304 Healthcare Software
d. NIST Framework for Improving Critical Infrastructure Cybersecurity, 2014
e. ISO/IEC 27001:20013 – Information Security Management
f. AAMI/ISO I4971 TIR in Process – AAMI Device Security Group
g. Medical IT Networks Safety, Security and Interoperability
h. IEC 80001-1 Managing Medical IT Networks and Relevant Technical Reports
i. TIR 80001-2-2:2012 – Application of Risk Management for IT Networks Incorporating Medical Devices

12:15 p.m. – 1:15 p.m. | **LUNCH**

1:15 p.m. – 2:15 p.m.

V. Risk Analysis for Medical Device Software

a. Preliminary hazard analysis
b. Top down analysis, Fault Tree Analysis
c. Bottom up analysis – design FMEA, function FMEA, process FMEA, use FMEA, common causes of software failures
d. Connectivity analysis between top down and bottom up

2:15 p.m. – 3:15 p.m.

VI. Group Exercise and Review With Instructors – Risk Analysis for Medical Device Mobile Apps

3:15 p.m. – 3:30 p.m. | **REFRESHMENT BREAK**

3:30 p.m. – 4:30 p.m.

VII. Risk Assessments and Risk Controls for Medical Device Software

a. Software related risk assessment
b. Risk control basics
c. Software lifecycle process control measures
d. Risk control identification
e. Control measures implementation and effectiveness

4:30 p.m. – 5:30 p.m.

VIII. Group Exercise and Review With Instructors – Risk Controls for Software Hazards

DAY TWO

8:00 a.m. – 8:30 a.m. | **CONTINENTAL BREAKFAST**

8:30 a.m. – 9:00 a.m.

IX. Latest Updates from FDA on Cybersecurity

a. Understanding the difference between software and hardware
b. Understanding software quality and reliability engineering
c. Challenges of software risk management and cybersecurity

9:00 a.m. – 10:00 a.m.

X. Cybersecurity Risk Analysis (Assets, Threats, Vulnerabilities)

a. Medical device cybersecurity basics
b. Asset profiling
c. Threat identification
d. Vulnerability identification
e. Software vulnerabilities
f. Attack Tree – top down and bottom up cybersecurity analysis
g. Connectivity between cybersecurity risk and safety risk

10:00 a.m. – 10:15 a.m. | **REFRESHMENT BREAK**

10:15 a.m. – 11:15 a.m.

XI. Group Exercise and Discussion With Instructors – Cybersecurity Risk Analysis

11:15 a.m. – 12:15 p.m.

XII. Cybersecurity Risk Assessments and Risk Controls

a. Cybersecurity risk assessment
b. Cybersecurity risk control basics
c. Software lifecycle process control measures
d. Cybersecurity capability and requirements identification
e. Special considerations for cybersecurity risk controls
f. Control measures implementation and effectiveness

12:15 p.m. – 1:15 p.m. | **LUNCH**

1:15 p.m. – 2:15 p.m.

XIII. Group Exercise and Discussion With Instructors – Cybersecurity Risk Assessments and Risk Controls

RITY RISK MANAGEMENT FOR MEDICAL DEVICES
ON AND BEST PRACTICES FOR COMPLIANCE

2:15 p.m. – 2:45 p.m.

XIV. Safety and Cybersecurity Risk Analysis Documentation for Stakeholders (FDA Reviewers, Hospitals, etc.)

a. Documentation for pre-market submission
b. Documentation for FDA inspection
c. Documentation for healthcare provider (e.g. hospitals)

2:45 p.m. – 3:15 p.m.

XV. Risk Management Completeness and Effectiveness – Introduction of Assurance Case Method

a. Limitations of current risk analysis methods
b. Assurance case concept
c. How assurance case method can help

3:15 a.m. – 3:30 a.m. | **REFRESHMENT BREAK**

3:30 p.m. – 4:00 p.m.

XVI. Safety and Cybersecurity Assurance Case Examples

a. Safety assurance case example for medical device
b. Security assurance case example

4:00 p.m. – 5:00 p.m.

XVII. Post-Market Safety and Cybersecurity Risk Management

a. Post market risk assessment and evaluation
b. MDR assessment
c. FDA recall classification — HHE
d. Legacy device cybersecurity risk management

5:00 p.m.

Workshop Adjournment

"All instructors were very knowledgeable and had expertise in the industry. Well done."

—May 2014 Workshop Participant

"The class had a good pace. It covered standard risk management well."

—May 2014 Workshop Participant

"[I liked the] small discussion groups and intimate setting"

—May 2014 Workshop Participant

WHO WILL BENEFIT

- Software systems design engineers and managers
- Quality, reliability and risk management engineers and managers
- Project managers involved in design and development
- Medical staff evaluating risk, safety or effectiveness
- Quality managers
- Regulatory affairs specialists and managers
- Medical device app developers
- IT systems development managers
- Contract manufacturers
- General/corporate counsel

MEET YOUR INSTRUCTORS

Fubin Wu is the Co-Founder of GessNet. GessNet is a software and consulting company specializing in medical device risk management (www.GessNet.com). He designed and led the development of TurboAC™ risk management and assurance case software, in concert with the FDA, Association for the Advancement of Medical Instrumentation (AAMI), medical device manufacturers, hospitals and industry experts. Mr. Wu has spent more than 16 years in medical device quality management systems, hardware/software reliability engineering and risk management, serving various roles from quality engineer to quality director.

Lisa Simone, PH. D., works for the FDA as Software Engineering Team Lead and Policy Advisor in the Office of Blood and Research and Review in the Center for Biologics Evaluation and Research (CBER). In this role she leads the software group in review of devices including blood donor screening tests, retroviral diagnostic tests, and software used to test, collect, process, or store donated blood. Dr. Simone also leads the development and review of policy for software in regulated devices.

COURSE BINDER MATERIALS

Each participant will receive a folder and flash drive packed with tools and reference materials in a combination of both electronic and hard copy format you can put to use right away, including:

- Copies of slides from PowerPoint presentations
- Preliminary hazard analysis example
- Fault Tree Analysis example, FMEA examples
- Example of connectivity between FMEAs and hazard analysis
- Risk Summary Traceability matrix example
- Cybersecurity risk analysis example – assets, threats, vulnerabilities analysis
- Safety assurance case example
- Cybersecurity assurance case example
- ISO 14971:2007 and EN ISO 14971:2012, IEC TR 80002-1 Application of ISO 14971 for Software
- IEC 62304 Medical Device Software Life Cycle Process - Risk Management Section
- Cybersecurity in Medical Devices (FDA Guidance, Oct 2014)
- NIST Framework for Improving Critical Infrastructure Cybersecurity (Version 1.0, 2014)
- Software-Related Recalls: An Analysis of Records (by Lisa K. Simone of FDA, AAMI BI&T Nov/Dec 2013 Issue)
- Best Practices in Applying Risk Management Terminology (by Fubin Wu and Alan Kusinitz, AAMI Horizons Spring 2015 Issue)
- Documenting Medical Device Risk Management through the Risk Traceability Summary (by Edwin Bills, Stan Mastrangelo, and Fubin Wu, AAMI Horizons Spring 2015 Issue)
- Reducing Risks and Recalls: Safety Assurance Cases for Medical Devices (by Sherman Eagles and Fubin Wu, AAMI BI&T Jan/Feb 2014 Issue)
- Hazard Analysis for a Generic Insulin Infusion Pump (by Yi Zhang, Paul Jones, and Raoul Jetley of FDA, J Diabetes Sci Technol. Mar 2010)
- Total Product Life Cycle: Infusion Pump (FDA Guidance, Dec 2014)
- IEC 80001-1 Managing Medical IT-Networks and relevant Technical Reports
- Radio Frequency Wireless Technology in Medical Devices (FDA guidance, August 2013)
- Mobile Medical Applications (FDA guidance, September 2013)
- Risk Management In the Design of Medical Device Software Systems (by Paul Jones PL, Biomed Instrum Technol 2002 Jul-Aug; 36(4):237-66)

FDANEWS PRESENTS THE

SOFTWARE AND CYBERSECURITY RISK MANAGEMENT FOR MEDICAL DEVICES

UNDERSTANDING THE FDA'S POSITION AND BEST PRACTICES FOR COMPLIANCE

LOCATIONS AND HOTEL ACCOMODATIONS

To reserve your room, call the hotel at the number below. Be sure to tell the hotel you're with the FDAnews workshop to qualify for the reduced rate. Only reservations made by the reservation cutoff date are offered the special rates, and space is limited. Hotels may run out of discounted rates before the reservation cutoff date. The discounted rate is also available two nights before and after the event based on availability. The hotel may require the first night's room deposit with tax. Room cancellations within 72 hours of the date of arrival or "no-shows" will be charged for the first night's room with tax.

LODGING AND CONFERENCE VENUE

Oct. 14-15, 2015

Hilton Washington DC/Rockville Hotel and Executive Meeting Center
1750 Rockville Pike, Rockville, MD 20852
Tel: +1 (301) 468-1100 • Toll free: (800) HILTONS
www.RockvilleHotel.com
Room rate: $215 plus 13% tax
Reservation cut-off date: Sept. 22, 2015

TUITION

Tuition rate is $1,797 per person and includes all workshop sessions, workshop materials, two breakfasts, two luncheons and daily refreshments.

TEAM DISCOUNTS

Significant tuition discounts are available for teams of two or more from the same company. You must register at the same time and provide a single payment to take advantage of the discount. Call +1 (703) 538-7600 for details.

CANCELLATIONS AND SUBSTITUTIONS

Written cancellations received at least 21 calendar days prior to the start date of the event will receive a refund -- less a $200 administration fee. No cancellations will be accepted -- nor refunds issued -- within 21 calendar days from the start date of the event. A credit for the amount paid may be transferred to any future FDAnews event. Substitutions may be made at any time. No-shows will be charged the full amount. In the event that FDAnews cancels the event, FDAnews is not responsible for any airfare, hotel, other costs or losses incurred by registrants. Some topics and speakers may be subject to change without notice.

FOUR EASY WAYS TO REGISTER

Online: www.fdanews.com/cybersecuritymd
Fax: +1 (703) 538-7676
Phone: Toll free (888) 838-5578 (inside the U.S.)
or +1 (703) 538-7600
Mail: FDAnews, 300 N. Washington St., Suite 200
Falls Church, VA 22046-3431 USA

Register Early — *Space Is Limited*

Hurry — register early because space is limited! Your tuition of $1,797 includes the two-day workshop, all workshop materials, continental breakfast each day and lunch on both days.

Payment is required by the date of the conference. We accept American Express, Visa and MasterCard. Make checks payable to FDAnews.

☑ **YES!** I want to attend **Software and Cybersecurity Risk Management for Medical Devices.** I understand the fee of $1,797 includes all workshop sessions, workshop materials, two breakfasts, two luncheons and daily refreshments. Please call (888) 838-5578 or fax to (703) 538-7676.

FDANEWS
300 N. Washington St., Suite 200
Falls Church, VA 22046-3431

Attendee 1: Name _____ Title _____ Email _____

Attendee 2: Name _____ Title _____ Email _____
(Please see "Team Discounts" above for tuition discounts when you send a team of two or more.) Email address (so you can receive order acknowledgements, updated news, product information and special offers)

Company Information

Organization _____

Address _____

City _____ State _____ Zip _____

Country _____

Phone _____ Fax _____

Payment Options

☐ Check enclosed, payable in U.S. funds to FDAnews

☐ Charge to: ☐ Visa ☐ MasterCard ☐ American Express

Credit card no. _____

Expiration date _____

Total amount $ _____

Signature _____
(Signature required on credit card and bill-me orders.)

Print name _____

☐ Bill me/my company $ _____

Purchase order # _____

(Payment is required by the date of the conference.)