JWG7 Tiger Team

Security & Privacy recommendations for ISO TC210, TC215 and IEC SC62A
Report out 2016-12-15
Charter for the JWG7 Security Tiger Team

1. **Consider how best to address security within the remit of the JWG7:**
   a) Safe, effective and secure health software and health IT systems, including those incorporating medical devices
   b) Standardization in the area of health informatics and electrical equipment in healthcare where ISO/TC 215 and IEC/SC 62A have identified a need for joint standards development.

2. **Consider how to leverage guidance (-2-2, -2-8 & -2-9)**

3. **What is directed toward the Design & Development "left" side (primary) stakeholders vs. Implementation & use "right" side (primary) stakeholders**

4. **Timing - 62304 and 80001-1 are both being revised and will be available before any new standard could be completed; so consider how near term updates could be included in these documents and published before any new documents - especially standards - could be completed and published.**

5. **Impact / use of current projects & documents: 82304-x, 62304, 81001-1, 80001-1 and 80001-2-x**

6. **Coordination with TC 210 & JWG1**

7. **Coordination with national initiatives, including in the EU, US and Asia**

8. **Consider recommendations to address privacy, and especially consent**
Recommendations

• The recommendations of the JWG7 tiger team is about how to extend risk management beyond safety for the new and upcoming document changes from JWG1 and JWG7.

• It does not provide all answers but mere guidance on how and where we need to ensure that Safety, Security and Privacy threats are considered in risk analysis and lifecycle management.
Introduction

• Global trends require us to make foundational changes in healthcare.
• These trends in healthcare require innovative solutions with a more multidisciplinary approach to be able to develop safe, effective and secure Health software and health IT systems, including those incorporating medical devices.
• The older functional safety standards did not address the challenges of highly connected “systems-of-systems”.
• ISO/IEC 80001-1 was a first attempt to address these risks related to “systems-of-systems” but new types of solutions and a change in the threat landscape and regulatory space requires a different approach.
1. Security Risk Management
   a) general
   b) for manufacturers
   c) for operators/users
2. Security Requirements to be met
3. Consistent set of terms
4. Software and System process requirements
   a) for manufacturers
   b) For operators/users
5. Communication between stakeholders
6. Data life cycle and Privacy
Main Takeaways

• Of key importance is the understanding that safety, security and privacy are interlinked and cannot be viewed in isolation!

• Update of 14791 → Extend beyond Safety
• Expanded (exploded) scope → Cloud, ByoMD, family portals
• Operational security → HDO is not the only operator/user
• “Multiple tiered suppliers” → Where SLAs won’t work anymore
• Privacy → Also consent and notification may introduce safety risks
• Consistent set of terms → Cyber, security, risk, threats, vulnerabilities
The JWG7 Tiger Team is looking forward to your feedback and questions.