AI SUMMIT
COLUMBUS, OH • OCTOBER 25–27, 2022

Update on Global AI/ML Regulatory and Standards Landscape

AI SUMMIT
COLUMBUS, OH • OCTOBER 25–27, 2022

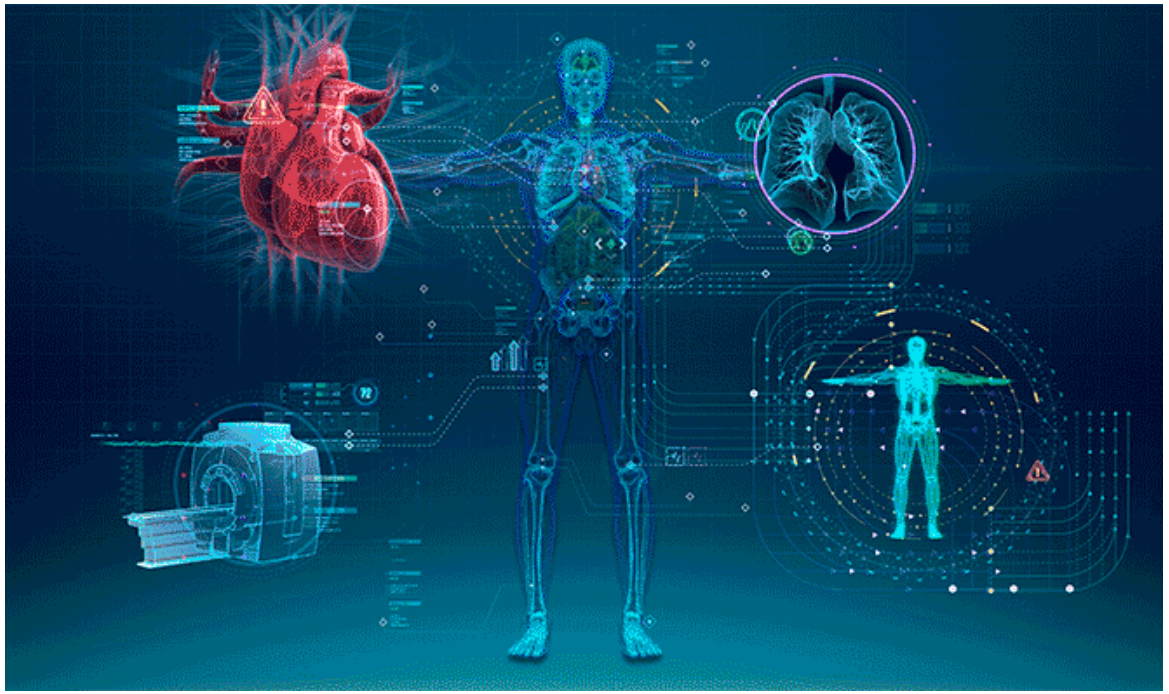
The Regulatory Landscape

Eric Henry

A Useful Model

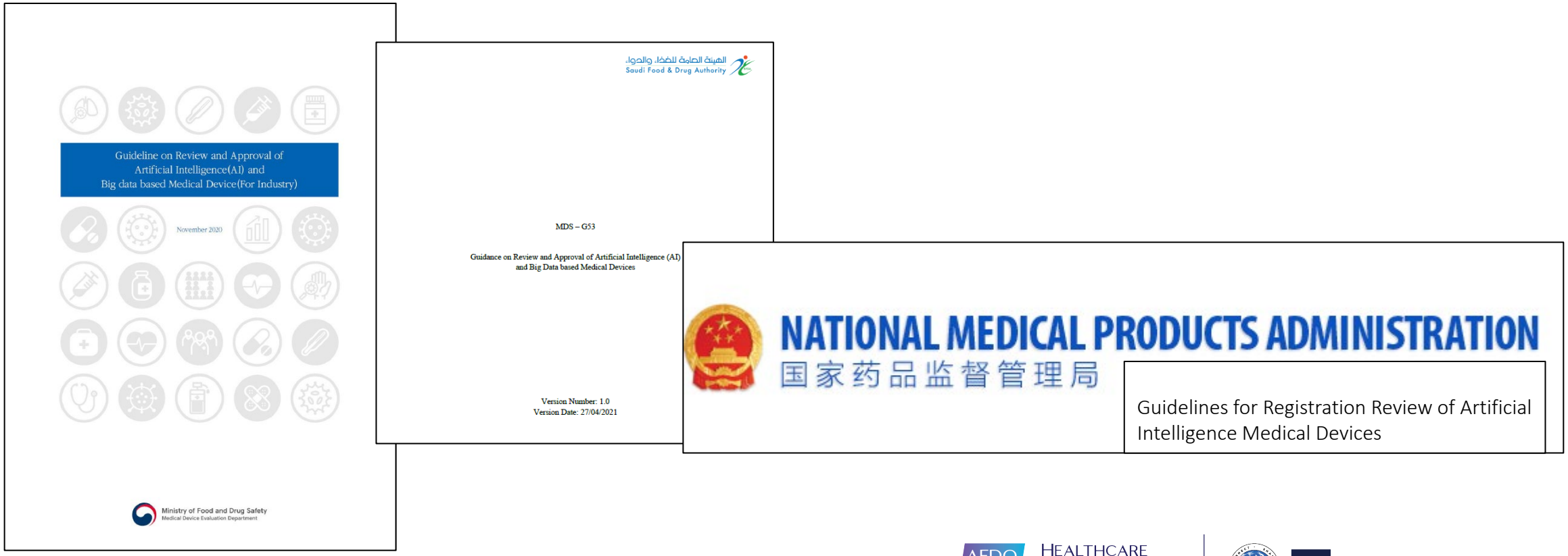
"All models are wrong, but some are useful."

-George E.P. Box-



AI SUMMIT
COLUMBUS, OH • OCTOBER 25–27, 2022

The Current Regulatory Landscape for AI/ML in the Life Sciences



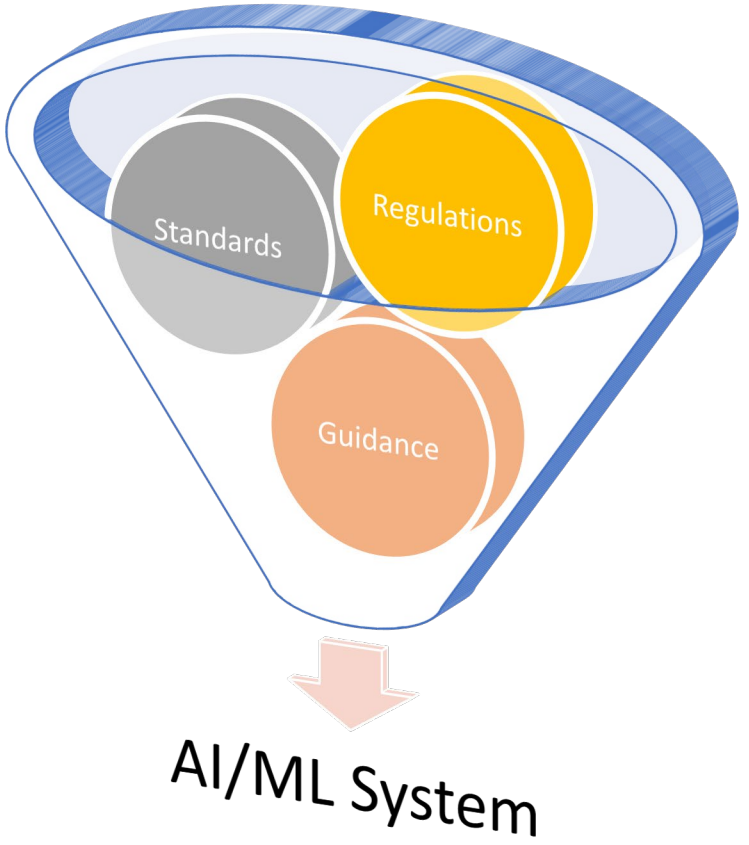
AFDO RAPS HEALTHCARE PRODUCTS COLLABORATIVE

Lots of Thinking

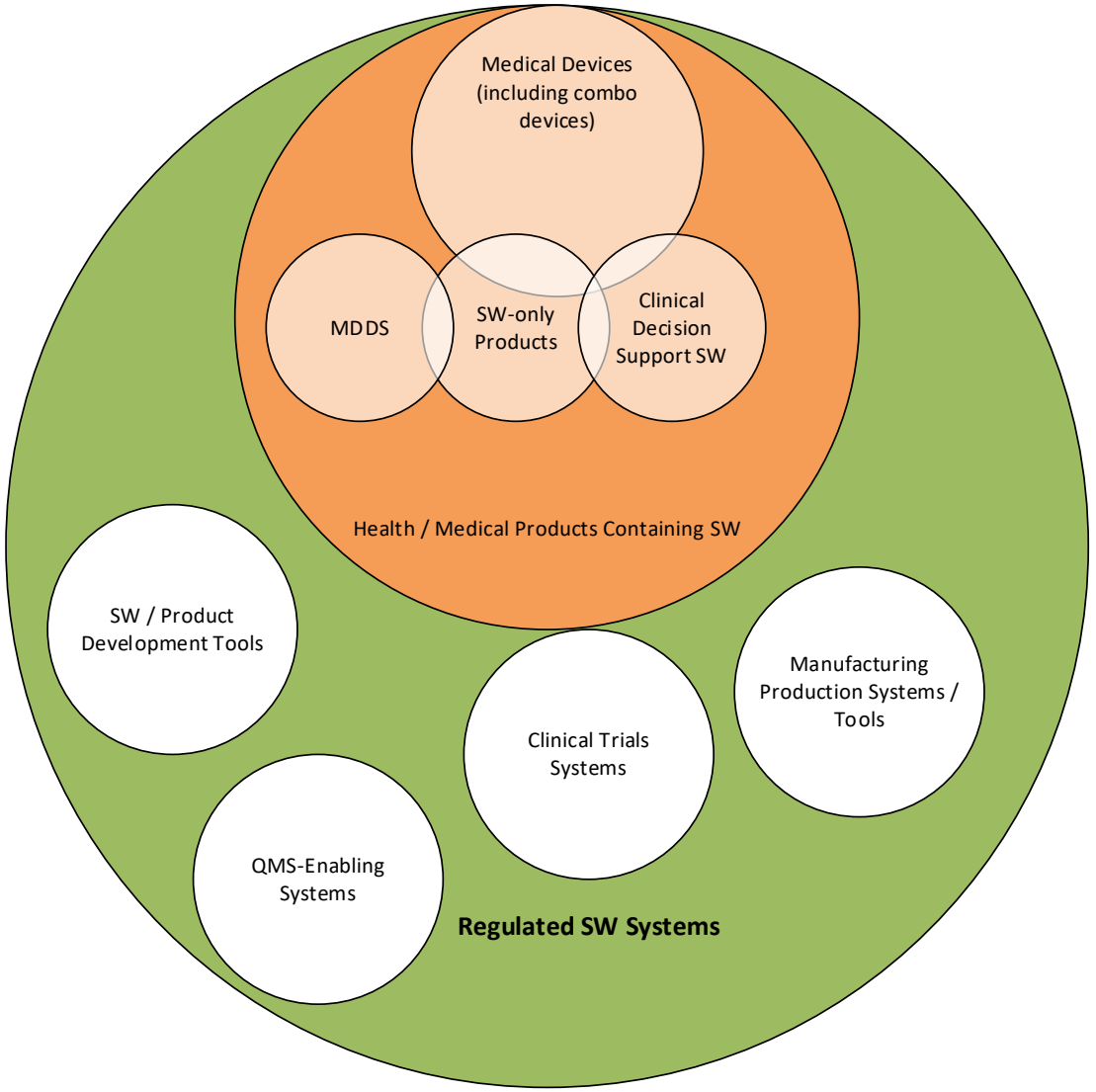
A Deeper Dive into the Chinese NMPA AI Guidance

- Locked algorithms only
- Methods and tools (including validation evidence) for:
  - Data capture
  - Data compilation
  - Data labeling
  - Data augmentation not allowed except for “adversarial sets,” which must be detailed
- Algorithm name, type, structure, input/output data types, flowcharts, programming framework, operating environment, and basis for selection
- Algorithm training methods
- Algorithm requirement specifications (including trace analysis)
- Comparative verification
- Verification and validation evidence
- Incorporation of other guidelines
  - Cybersecurity
  - Mobile medical device
  - Medical device software
  - Human factors
- AI chip names, models, specifications, manufacturer, performance indicator, and “other information”
- Risk management dossier
- Use of third-party databases for validation (6 requirements)

Using Existing Frameworks



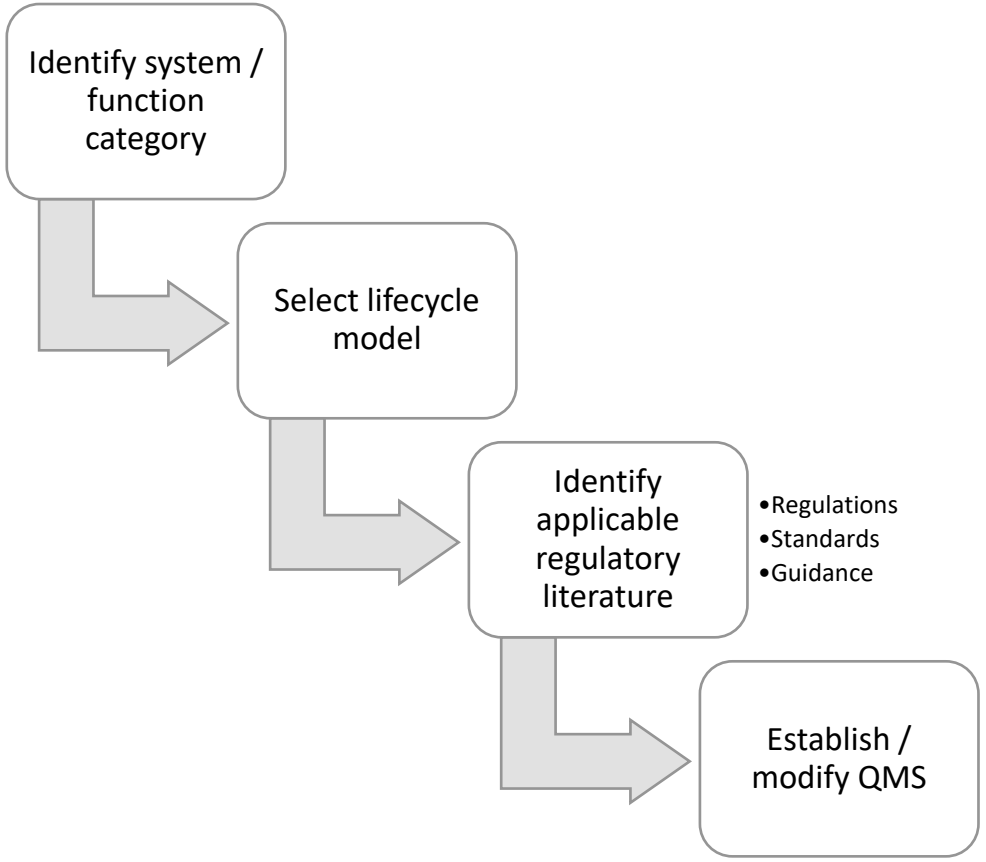
Know Thyself



A Multipurpose Tool

Two Primary Purposes:

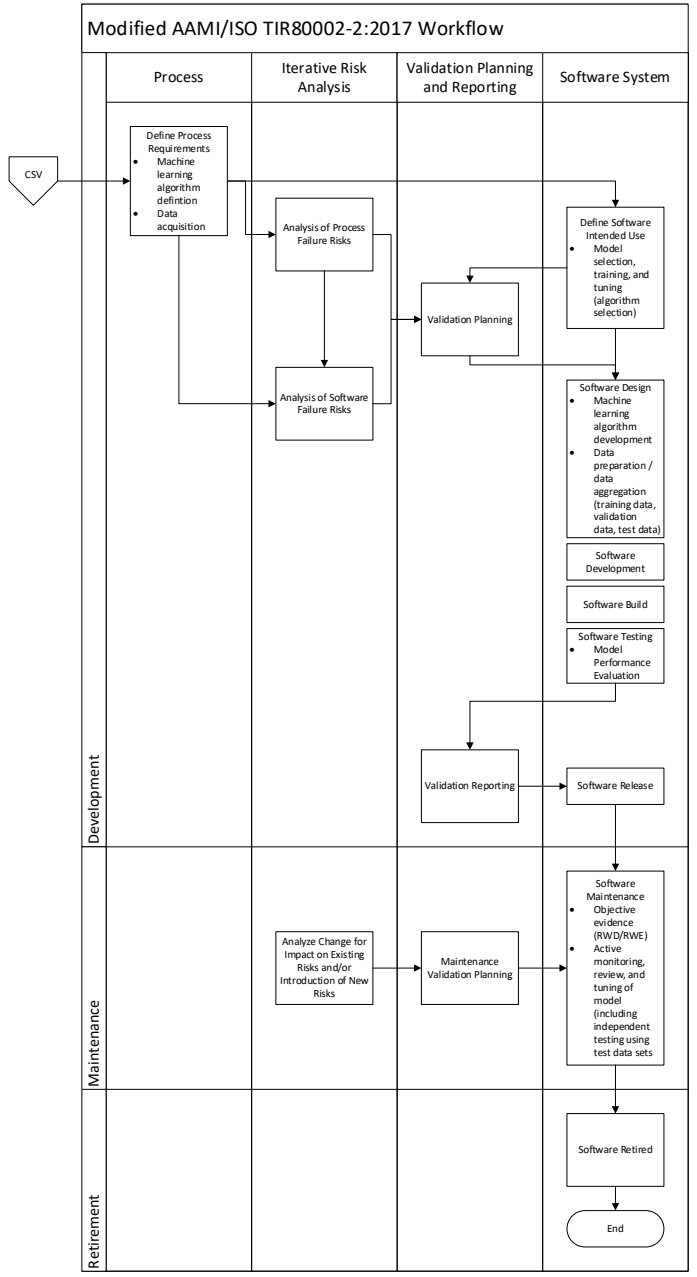
- Choose a lifecycle model applicable to the system
- Identify applicable regulatory literature as the basis for the Quality Management System (QMS)



AI SUMMIT
COLUMBUS, OH • OCTOBER 25–27, 2022

Non-Product Categories: Non-Manufacturing Systems

- Based on AAMI/ISO TIR80002-2:2017
- Clinical Trials Systems
  - Data analytics
- Software / Product Development Tools
  - AI modeling
  - Defect management
  - NLP tools
- QMS-Enabling Systems
  - Complaint management / analysis
  - CAPA management / analysis



AFDO RAPS HEALTHCARE PRODUCTS COLLABORATIVE

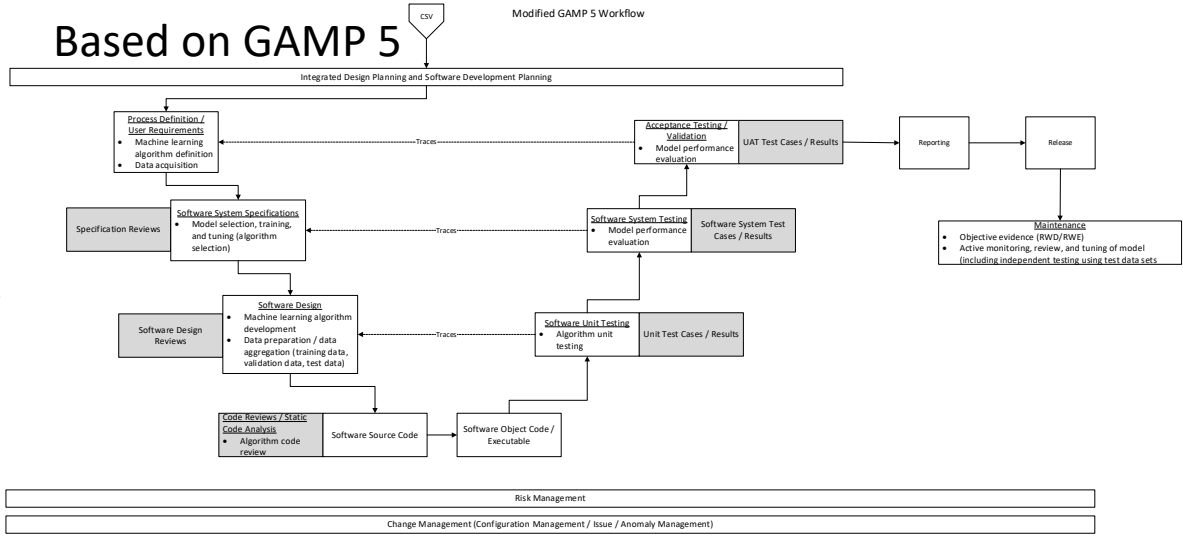
Non-Product Categories: Manufacturing Systems

Pharmaceutical Manufacturing

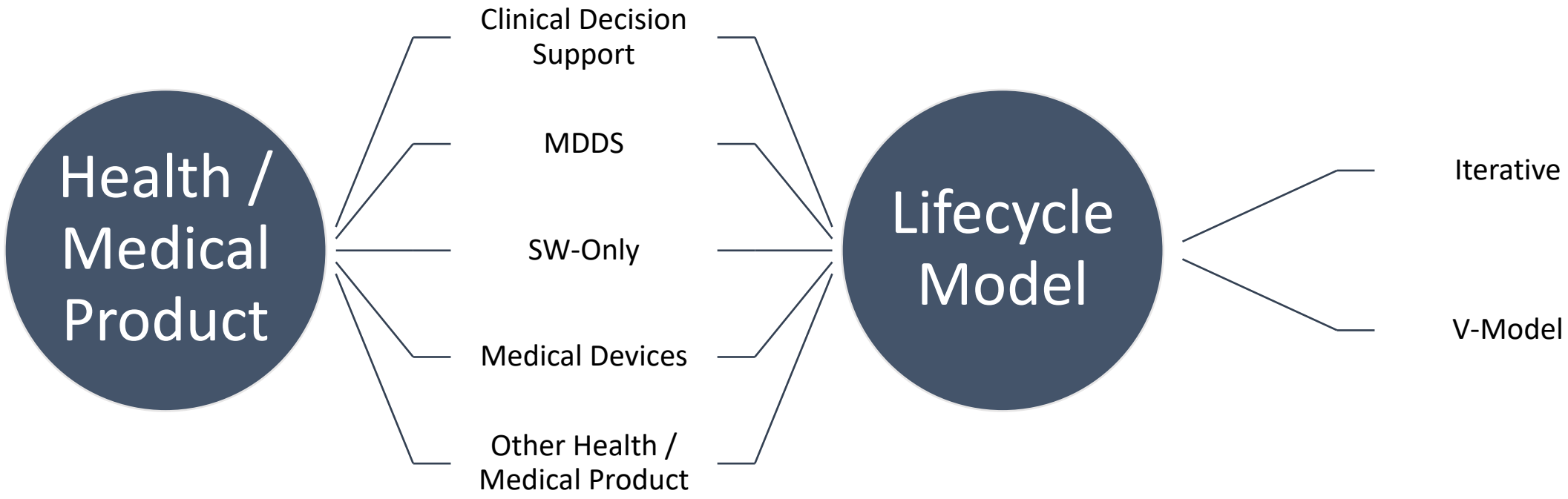
Medical Device Manufacturing

Manufacturing Computer Software Validation (CSV)

Based on GAMP 5



Product Categories



AI SUMMIT
COLUMBUS, OH • OCTOBER 25–27, 2022

The Standards Landscape

Pat Baird

Why do we need standards? One reason: We forget items that are second nature to us

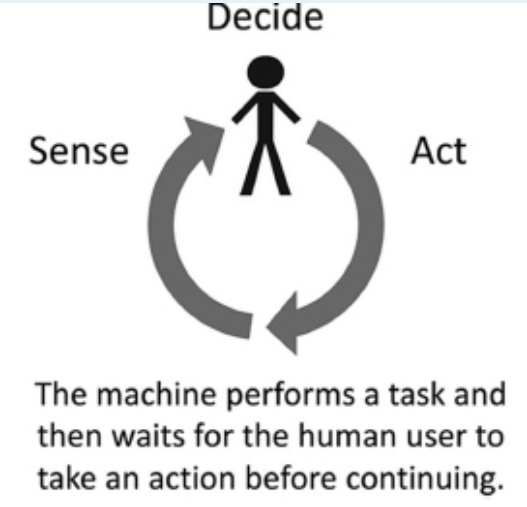
- Draft UL standard on fully-autonomous vehicles: what does the vehicle do when approaching a stoplight that just turned yellow?
- Defeating facial recognition software
- Defeating speed limit sign

https://www.businessinsider.com/hackers-trick-tesla-accelerating-85mph-using-tape-2020-2

Takeaway: we are in an age of "Narrow AI"

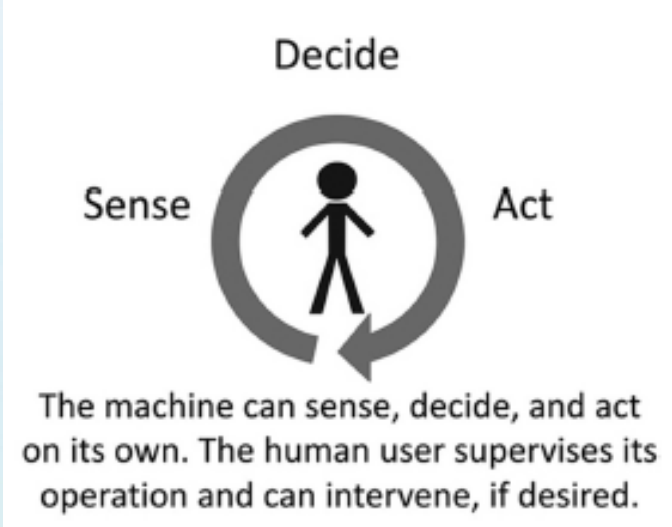
To what degree do we need "humans in the loop" ?

First level needs a human to complete the task



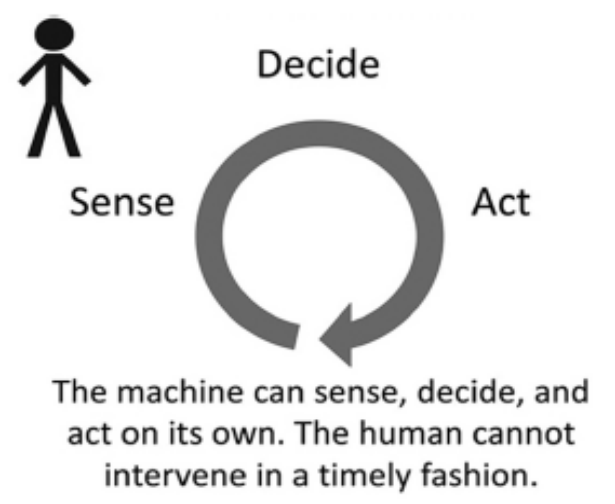
The machine performs a task and then waits for the human user to take an action before continuing.

Second level allows for human over-ride



The machine can sense, decide, and act on its own. The human user supervises its operation and can intervene, if desired.

Third level does not allow for intervention



The machine can sense, decide, and act on its own. The human cannot intervene in a timely fashion.

The International Medical Device Regulators Forum published a framework for assessing the risk of (non-AI) SaMD, according to the significance of the software when making decisions, and the criticality of the patient state

State of Healthcare situation or condition	Significance of information provided by SaMD to healthcare decision		
	Treat or diagnose	Drive clinical management	Inform clinical management
Critical	IV	III	II
Serious	III	II	I
Non-serious	II	I	I

IMDRF "Software as a Medical Device: Possible Framework for Risk Categorization and Corresponding Considerations"

For AI, I think that "Treat or diagnose" has several levels, depending on how much freedom the AI is given – does the human have to "approve" before action is taken or does human have the ability to "override".

This has been included in CTA standards, is being considered by WHO, and has been adopted by AMA's payment codes.

State of Healthcare situation or condition	Significance of information provided by SaMD to healthcare decision				
	Treat or diagnose w/ no intervention possible	*Treat or diagnose w/Override*	Treat or diagnose *w/Approval*	Drive clinical Management	Inform clinical Management
Critical	???	??	IV	III	II
Serious	??	IV?	III	II	I
Non-serious	IV?	III	II	I	I
	Automated/Autonomous Intelligence			Assistive Intelligence	

Standards Overview

There isn't much that is already published, but there are several efforts that I'll be talking about:

- ISO/IEC JTC1, SC42, developing horizontal standards for all industries. Many simultaneous projects and even more are being created. Not likely that these horizontal standards would be required for medical devices, but they may contain ideas that we like and would carry to healthcare.
- ISO/IEC TC215 (health software standards like 62304, 82304, 80001-x series, + 200 more standards) has created Task Force 5 not to write standards, but to provide some support for people wanting to write standards – a landscape of various projects, develop use cases, do some education, liaisons, etc.
- IEEE also developing a number of AI standards, but only a few are specific to healthcare.
- CTA is developing general AI standards as well as healthcare-specific AI standards.
- AAMI & BSI have also started an AI standards committee.

AI SUMMIT
COLUMBUS, OH • OCTOBER 25–27, 2022

ISO/IEC JTC1 SC42 – Standards for all Industries

Structure:
WG1 – Foundational standards (terminology, framewc
WG2 – Big Data (vocabulary, reference architecture)
WG3 – Trustworthiness (incl. risk, robustness, bias)
WG4 – Use cases and applications
WG5 – Computational approaches & characteristics of

JWG1 (SC40)– Governance implications of AI
JWG2 (SC7) – Testing of AI-based systems
AG1 – Management Systems Standard
AG2 – AI Systems Engineering
AG3 – AI standardization roadmapping

AFDO RAPS HEALTHCARE PRODUCTS COLLABORATIVE

AFDO RAPS

4213 - Information technology — Artificial Intelligence — Assessment of machine learning classification performance
4213 - Assessment of machine learning classification performance
5338 - AI system life cycle processes
5339 - Guidelines for AI applications
5392 - Information technology — Artificial intelligence — Reference architecture of knowledge engineering
5469 - Functional Safety
5471 - Artificial intelligence — Quality evaluation guidelines for AI systems
6254 - Objectives and methods for explainability of ML models and AI systems
8200 - Controllability of automated artificial intelligence systems
12791 - Treatment of unwanted bias in classification
12792 - Transparency taxonomy of AI systems
20546 - Big Data - Overview and Vocabulary
20547.1 - Big Data reference architecture - Part 1: Framework and application process
20547.2 - Big Data reference architecture - Part 2: Use cases and derived requirements
20547.3 - Big Data reference architecture - Part 3: Reference architecture
20547.4 - Information technology — Big data reference architecture — Part 4: Security and privacy
20547.5 - Big Data reference architecture - Part 5: Standards roadmap
22989 - AI Concepts and Terminology
23053 - Framework for AI using ML
23894 - Risk Management (ISO 31000, not 14971)
24027 - Bias in AI systems and AI aided decision making
24028 - Overview of Trustworthiness in AI
24029.1 - Assessment of the robustness of neural networks - Part 1 Overview
24029.2 - Formal methods methodology
24030 - Use cases and application
24368 - Overview of ethical and societal concerns
24372 - Overview of computations approaches for AI systems
24668 - Process management framework for Big data analytics
25059 - Systems and software Quality Requirements and Evaluation (SQuaRE)
38507 - Goveranance implications of the use of AI by organizations.
42001 - Management system
22100-5 - Safety of machinery — Relationship with ISO 12100 — Part 5: Implications of artificial intelligence machine learning
5259-1 - Data quality for analytics and ML — Part 1: Overview, terminology, and examples
5259-2 - Data quality for analytics and ML — Part 2: Data quality measures
5259-3 - Data quality for analytics and ML — Part 3: Data Quality Management Requirements and Guidelines
5259-4 - Data quality for analytics and ML — Part 4: Data quality process framework

ISO/IEC JTC1 SC42

has a lot of projects..

- Some of these topics are not what you think -- note that “risk management” is enterprise-risk, not safety-risk. If you want safety, look at 5469
- Some new projects include “Oversight”; another is exploring the positive use-cases for AI applications.
- Also be aware that some legislators assume that horizontal standards can apply to all industry – after all, they are horizontal!

IEEE

IEEE also has multiple (horizontal) AI standards, as well as a few specific to healthcare:

P2801 Recommended Practice for the Quality Management of Datasets for Medical Artificial Intelligence Recommendation

P2802 Standard for the Performance and Safety Evaluation of Artificial Intelligence Based Medical Device: Terminology

And although it's not healthcare-specific…

P7003 Algorithmic Bias Considerations

TC215 Task Force 5: AI Stuff!

- In 2019, ISO/TC215 created an Ad Hoc Group (AHG2) on Application of AI in Health Informatics; the resulting report had over 30 recommendations so TC215 formed TF5 to implement the recommendations, including:
  - Create (and maintain) a standards landscape so that TC215 knows what other teams are working on.
  - Setup collaborations with other organizations
  - Develop common definitions for TC215 teams to use
- The idea is not to have TF5 write standards, but for them to provide infrastructure to help with future standards.

IEC TC62 Software Network and Artificial Intelligence advisory Group (SNAIG)

- TC62 formed a group to make recommendations about what standards might need to be updated or created. Their final report will be discussed in an upcoming TC62 Plenary meeting.
- The group came up with a process for identifying and prioritizing future projects – this was not simply a collection of people's opinions.

IEC/TC62 PT 63450 AI-enabled Medical Devices – Methods for the Technical Verification and Validation

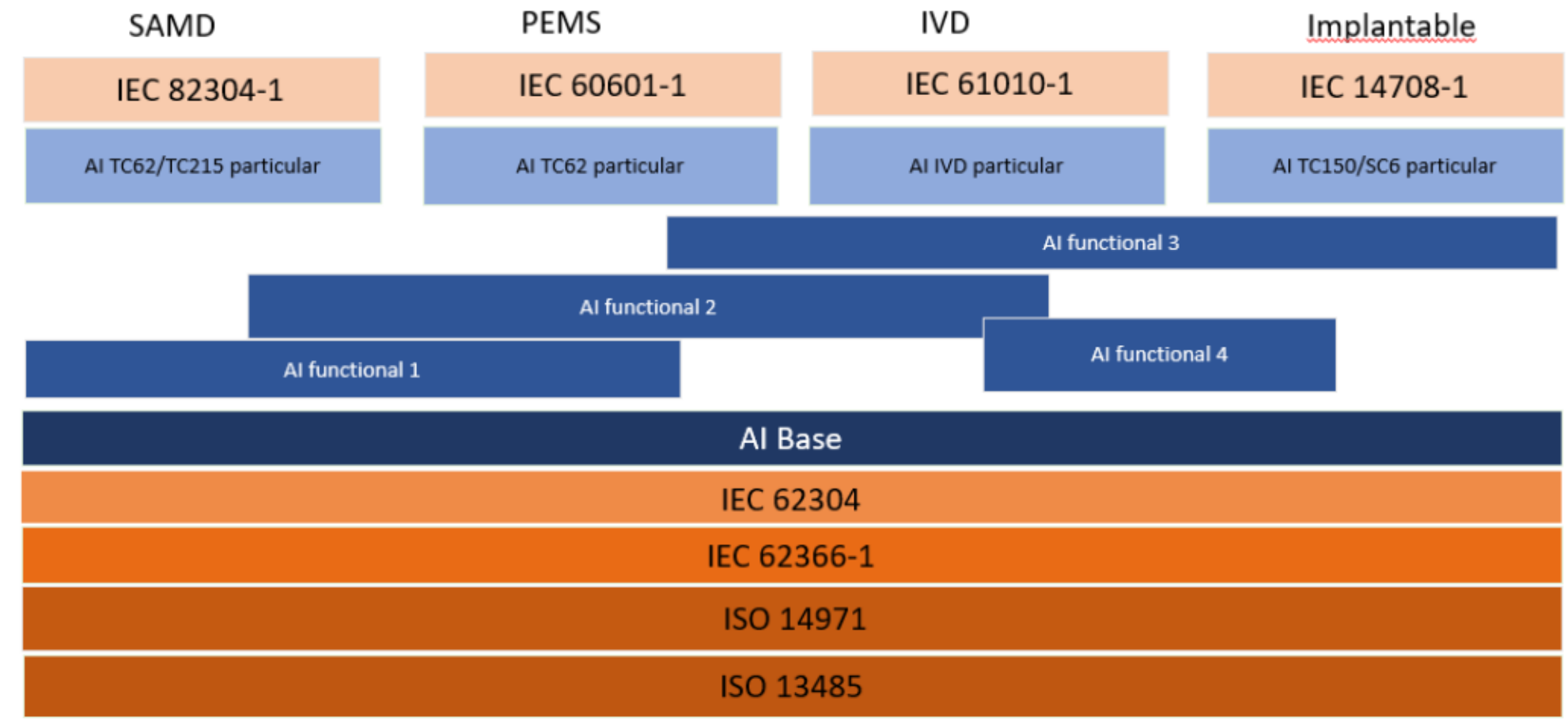
"This document establishes methods for medical device manufacturers to **verify and validate** artificial intelligence / machine learning-enabled medical devices (AI/ML-MD), i.e. medical devices that use artificial intelligence, in part or in whole, to achieve their intended medical purpose. This includes verification and validation activities for the **model** of the artificial intelligence as well as **selection**, **metrological characterization** and **management** of the **data sets**.

Such activities are implemented at **various stages of the medical device lifecycle**, especially including design control, monitoring and design change.

This document is also applicable to any hardware or software utilizing artificial intelligence that impacts the intended use of a medical device"

The basic idea is a three-fold architecture (see Figure 1) based on:

- a common **AI Base Level*** applying to all AI-enabled medical devices (e.g., bias management, Testing of ML-enabled Medical Devices); and
- Specific AI aspect applying to a group of AI-enabled medical devices (**functional***) (e.g., image analysis, waveform analysis); and
- AI methods or measures specific to intended purpose (**particulars***) (e.g., 2D x-ray for dentistry, tongue image analysis (ISO 20498-1)) documents.



IEC TC62 should consider preparing NPs regarding the following standardization fields in green in Figure 2.

Overview			
Existing standards sufficient; some additions for the application to AI-MD software different partners			
(all sorts of MD) QMS, RMS, PMS, Security, Privacy	Clarification where additional factors are to be considered - basic standards are basically sufficient		Impact of patient as operator in the private space and cloud are hardly considered at present
Traditional ME (Hardware + non AI Software)	covered		
SAMD	Extension/addition to 62304 for ML	clinical validation for SAMD	
New standards are necessary; IEC TC62 is in the lead or works in a JWG with partners			
(ML – MD, maybe AI - MD in general) Logic component	Quality metrics for external data component	clinical validation (data aspects, statistical effectiveness)	Techno-Vigilance necessary
	Quality criteria and docu req. for „logic" component		Clinical utility (effective benefit at the site)
	Methods for building test sets		Transparency in Usage and operation
(AI – MD) Bias (Ethics?)	Overarching process standard and consideration in all columns for symbolic AI + ML		
New standards are necessary; ISO TC215 is in the lead or works in JWGs; IEC TC 62 contributes			
(ML – MD) Data component	Data Lifecycle process standard (incl. Selection, collection, vetting, documentation etc.)		
	Quality standards in design and development		Including changes based on PMS data or continuous learning
	Quality assurance methods and quality metrics		
	Methods for validation		

Figure 2: Proposed IEC/ISO cooperation for AI/ML Medical Device Standards

Possible projects for TC62 or JWG

- ISO/IEC Develop a standard for documentation requirements providing evidence of the fulfullment of quality criteria
- Methods to build training and test sets from available data
- Clinical validation (might be handled elsewhere)
- Techno-vigilance (post-Market surveillance, but no concrete recommendations right now)
- Transparency (e.g. compliance, explainability, trustworthiness, etc.)
- Bias management (monitor SC42 TR 24027)
- Security

Possible Collaboration with TC210

- Addition to ISO 13485 Quality Management
- Addition to ISO 14971 Risk Management
- Addition to ISO TR 20416 Post-market Surveillance
- Addition to ISO 20417 information supplied by manufacturer
- Addition to IEC 62366-1 Usability
- Collaborative work for bias management…

Possible Collaboration with TC215

- Quality criteria and metrics for the data used
- Terminology

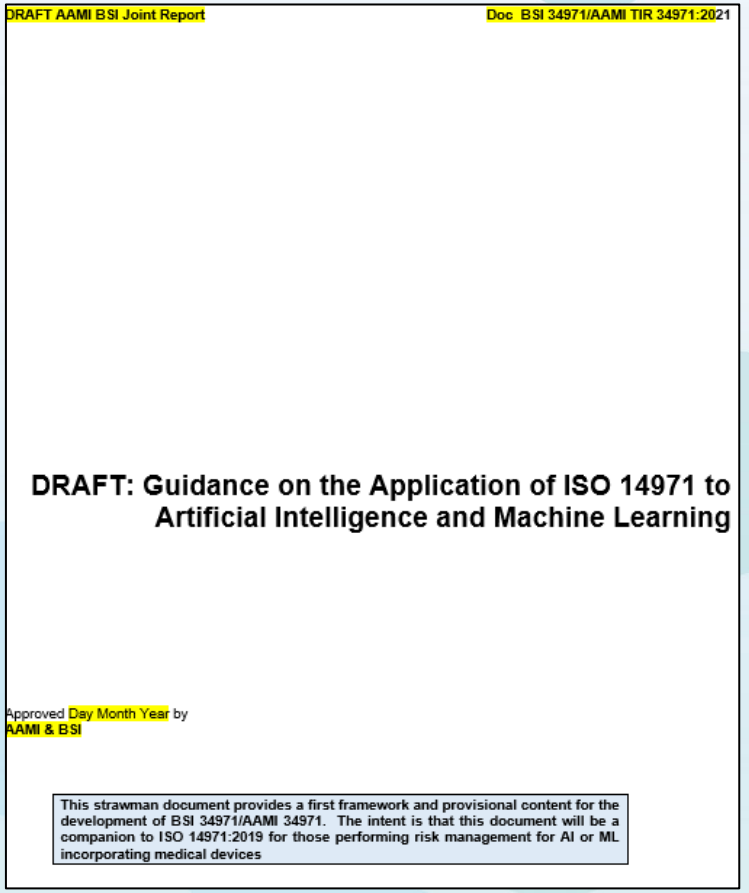
AAMI/BSI Standards Collaboration

After publishing a few whitepapers with BSI, AAMI/BSI started working on another whitepaper regarding AI risk management. Feedback we received on the whitepaper was “why are you doing another whitepaper? A standard or a TIR would be more useful…”

An official AI committee was formed, and the first project is TIR 34971 – Guidance on the Application of ISO14971 to Artificial Intelligence and Machine Learning.

You might remember that the ISO/IEC 24971 provides guidance on how to implement 14971, and includes an annex of special considerations for IVDs. The risk management process is the same, but there are some things you might not have considered when it comes to IVD risk management.

34971 is following that same pattern – the process is the same, but there are new ways to fail. There are different things to look for (e.g. bias), there are different risk controls to consider.


DRAFT AAMI BSI Joint Report

Doc BSI 34971/AAMI TIR 34971:2021

DRAFT: Guidance on the Application of ISO 14971 to Artificial Intelligence and Machine Learning

Approved Day Month Year by
AAMI & BSI

This strawman document provides a first framework and provisional content for the development of BSI 34971/AAMI 34971. The intent is that this document will be a companion to ISO 14971:2019 for those performing risk management for AI or ML incorporating medical devices

Consumer Technology Association (CTA)

CTA is the trade association for the consumer technology industry (all consumer industries – not just healthcare)

Established AI working group, published two whitepapers in 2018 – general introduction & use cases.

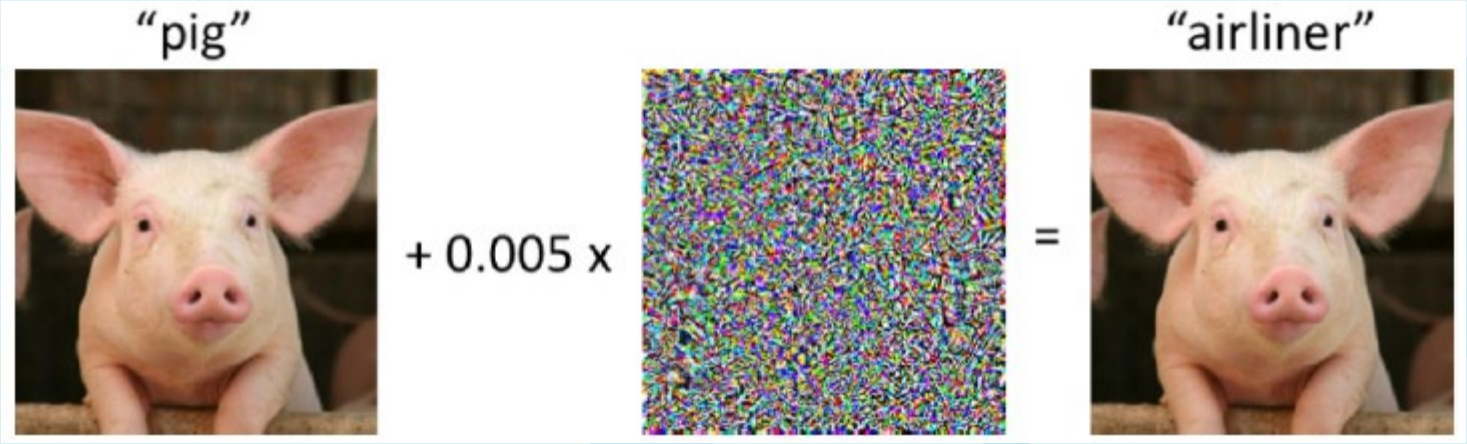
AI standards committee (R13) & Health Care working group (R13 WG1). Publications include:

- "Definitions / Characteristics of AI in Health Care (ANSI/CTA-2089.1)"
- "The Use of AI in Health Care: Trustworthiness (ANSI/CTA-2090)"
- "The Use of AI in Health Care: Managing, Characterizing, and Safeguarding Data"

Current project is about Bias Management

Cybersecurity!

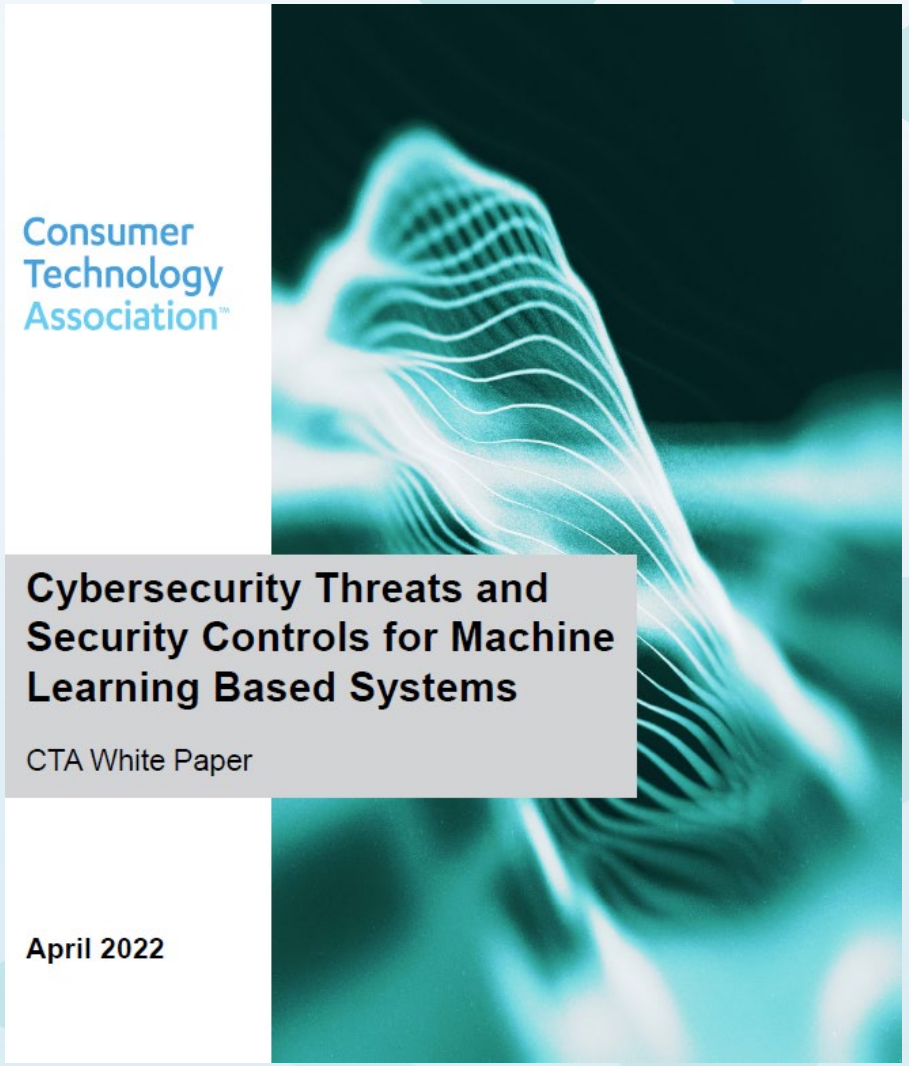
- ML systems have a lot of data. Potentially very attractive data. This data is often handled by multiple stakeholders as it is passed from one system to another.
- Due to the nature of the data & how ML systems work, it might not be obvious that there has been a security issues…



“Example of adversarial perturbation used to evade classifiers”;
Draft NISTIR 8269 A Taxonomy and Terminology of Adversarial Machine Learning

Cybersecurity!

- Standards organizations are starting to recognize that this is an issue and have started some projects to address it.
- CTA has published a whitepaper; this generated enough interest that they are currently working on a standard.
- ISO/IEC SC27 & SC42 have joined forces to work on an international standard for security of ML systems; however, this is a horizontal standard across all sectors – I am hoping that we can have an informative annex that addresses some of the unique considerations that we have in healthcare.



Questions?