FORUM
Academy of Medical Sciences

ROYAL ACADEMY OF ENGINEERING

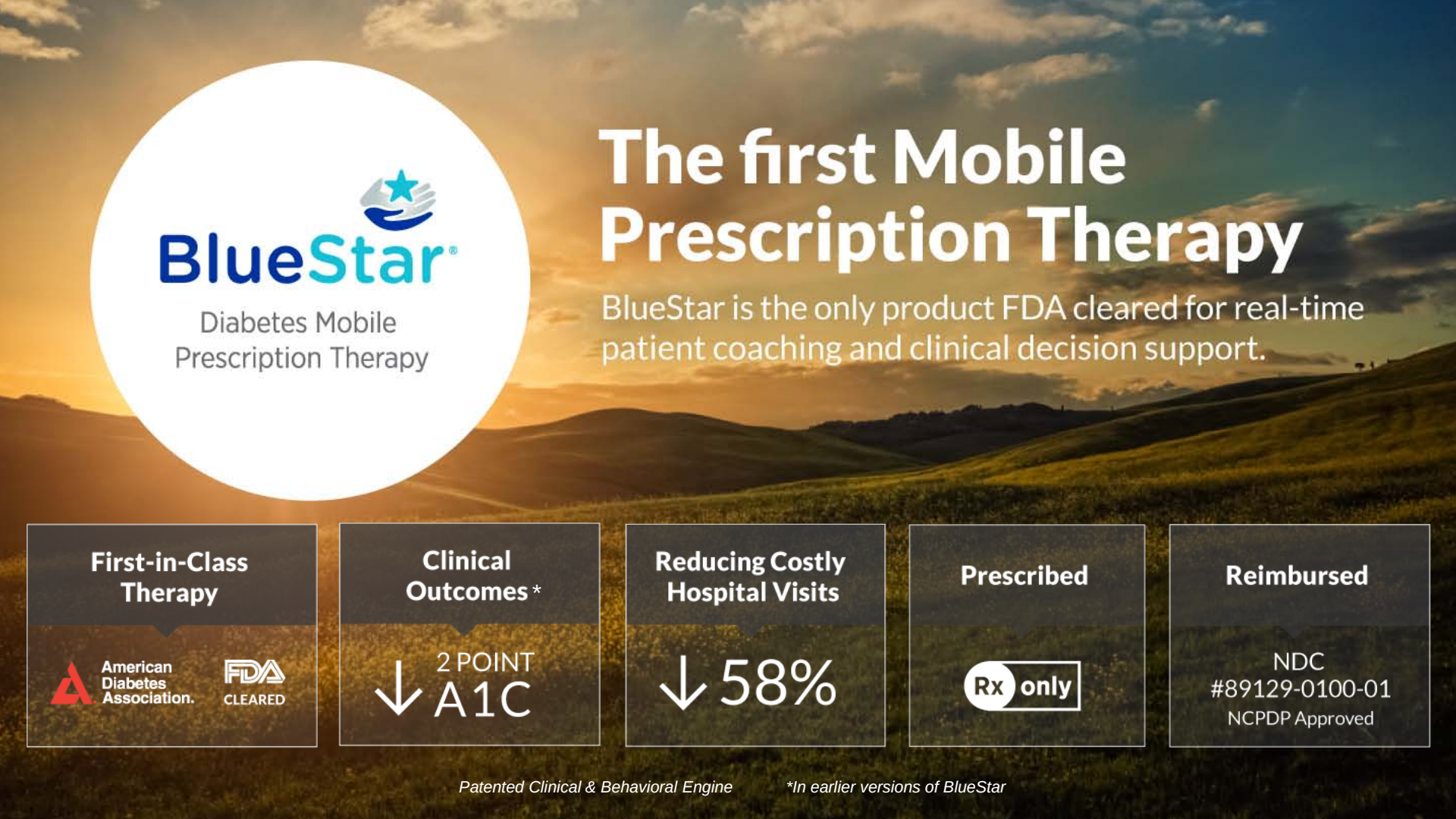
Health apps: regulation and quality control

Wednesday 19 November 2014, Academy of Medical Sciences

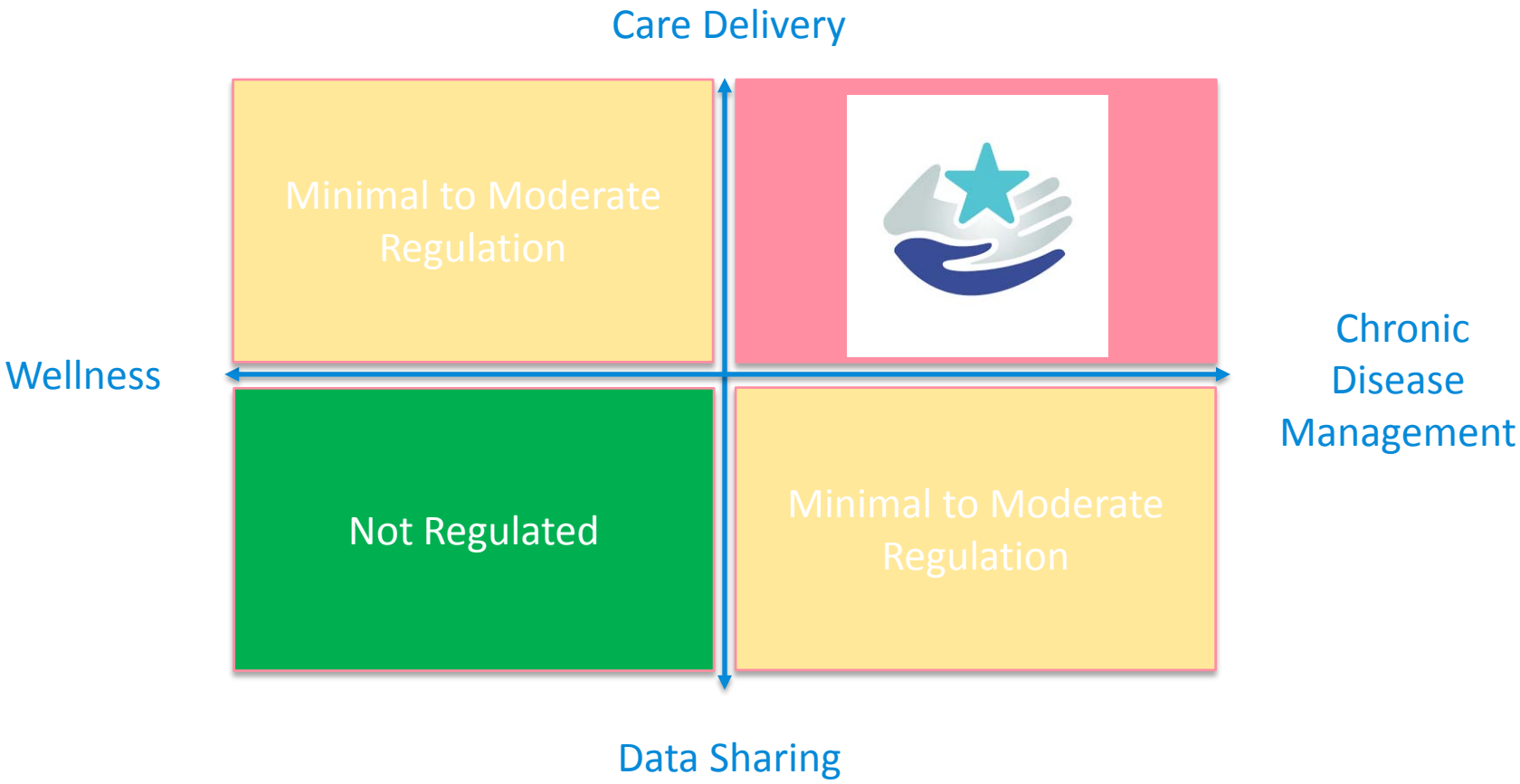
Developing the first CE-marked medical app: Mersey Burns

Rowan Pritchard Jones
Department of Burns and Plastic Surgery, Whiston Hospital

Available from: https://prezi.com/boyb9fhskpno/academy-med-sci/


BlueStar®
Diabetes Mobile
Prescription Therapy
The first Mobile Prescription Therapy
BlueStar is the only product FDA cleared for real-time patient coaching and clinical decision support.
First-in-Class Therapy
American Diabetes Association.
FDA CLEARED
Clinical Outcomes *
↓ 2 POINT A1C
Reducing Costly Hospital Visits
↓ 58%
Prescribed
Rx only
Reimbursed
NDC #89129-0100-01
NCPDP Approved
Patented Clinical & Behavioral Engine
*In earlier versions of BlueStar

Digital Health Landscape



Managing Chronic Disease Can Be Daunting

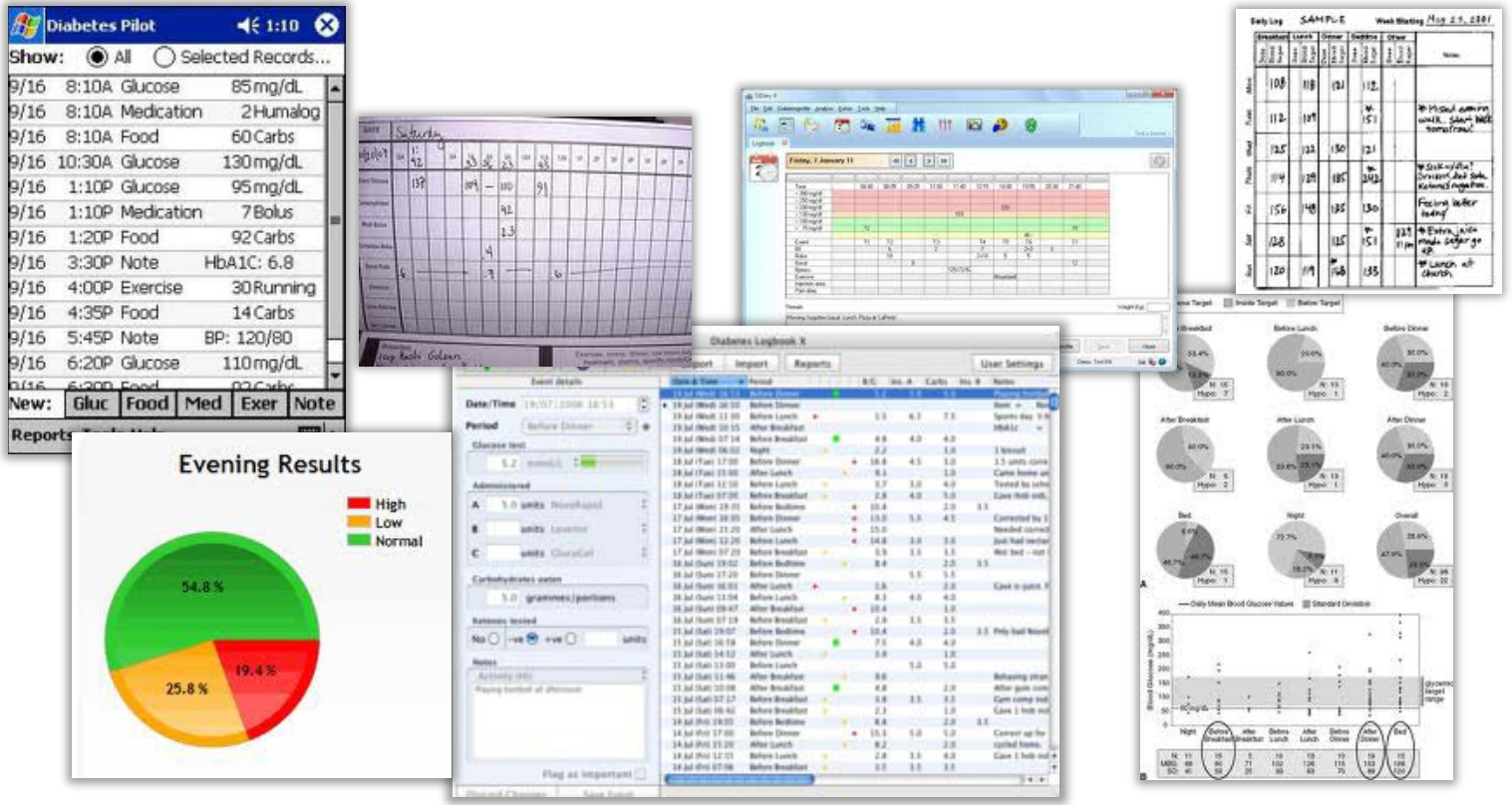
Healthcare
Four, 15-minute doctor visits a year

Therapeutics
Average of 9 prescriptions yearly

Self-Management
48 minutes a managing disease(s)

A Small Thing Called “Life”
8,766 hours a year balancing life
and a chronic disease

Raw Data Isn't Necessarily the Answer

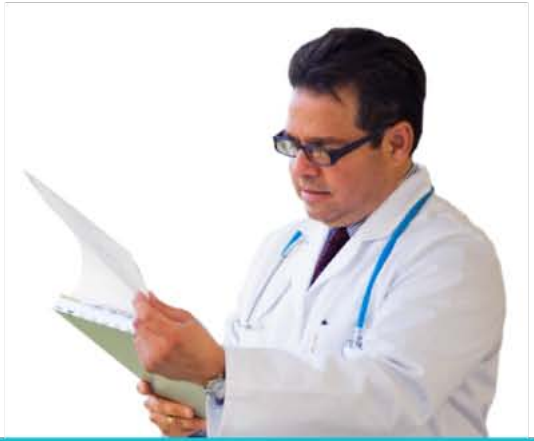


What if We Could Transform the Data?

To Deliver Actionable Knowledge…

Diabetes Care, Anytime Anywhere

24/7, automated, real-time guidance and education.



Optimizing Clinical Decisions

Treatment and quality recommendations based on evidence-based guidelines for healthcare providers.

Seamless, End-to-end Deployment*

Provider In-Servicing

Face-to-face physician detailing.

Patient Training

Patients are trained face-to-face or remotely.

Customer Care

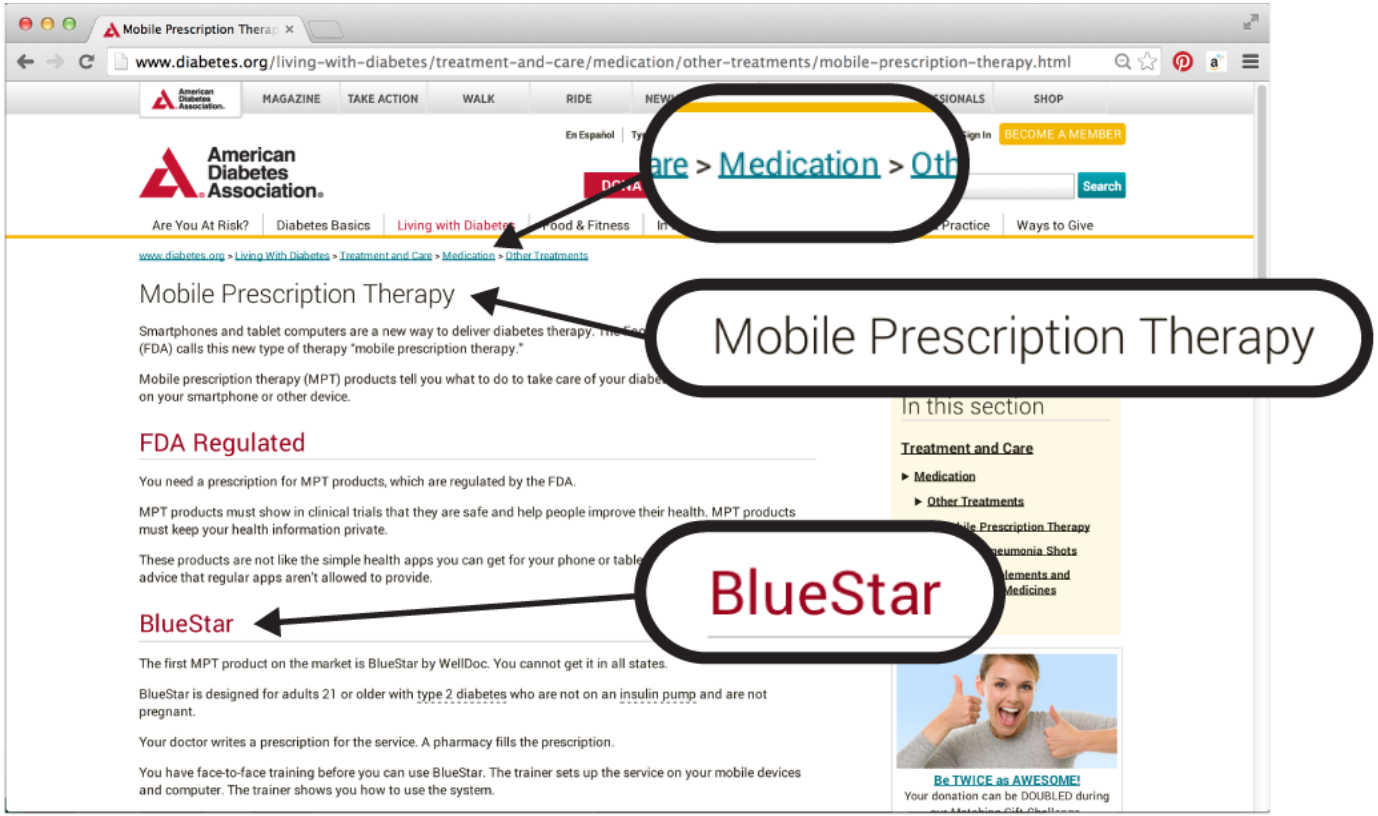
Product support for patients & providers.

Nationwide Pharmacy Dispensing

Rx only

NDC #89129-0100-01

ADA Recognized as New Type 2 Medication



Source: ADA www.diabetes.org

Potential Regulatory Framework for mHealth

Layer 1: Users	Stakeholders who use the system throughout the solution's lifecycle
Layer 2: Application	The feature set and attributes of the software solution that is deployed
Layer 3: Environment	The physical, regulatory, and security elements of both the mobile and EHR software
Layer 4: Devices	The end user mobile Internet devices or hardware that are being used (e.g., cellphones, computers) to deliver the MIT solution and their unique attributes
Layer 5: Network connectivity	The properties of the interfaces that must be considered to ensure proper persistence, resilience, and availability to support integration
Layer 6: Services	Awareness, education, and training required to ensure maximum value to all users
Layer 7: Core integration	The data standards, data mapping, and application/systems/workflow integration
Layer 8: Operating model	The operating and business aspects of the project, including industry observations, cross-enterprise collaboration, and open innovation

Regulation and oversight for developing embedded medical software

Academy of Medical Sciences/Royal Academy of Engineering
Joint meeting on 'Health apps: regulation and quality control'

Dr Chris Elliott FREng

Leman Micro Devices SA

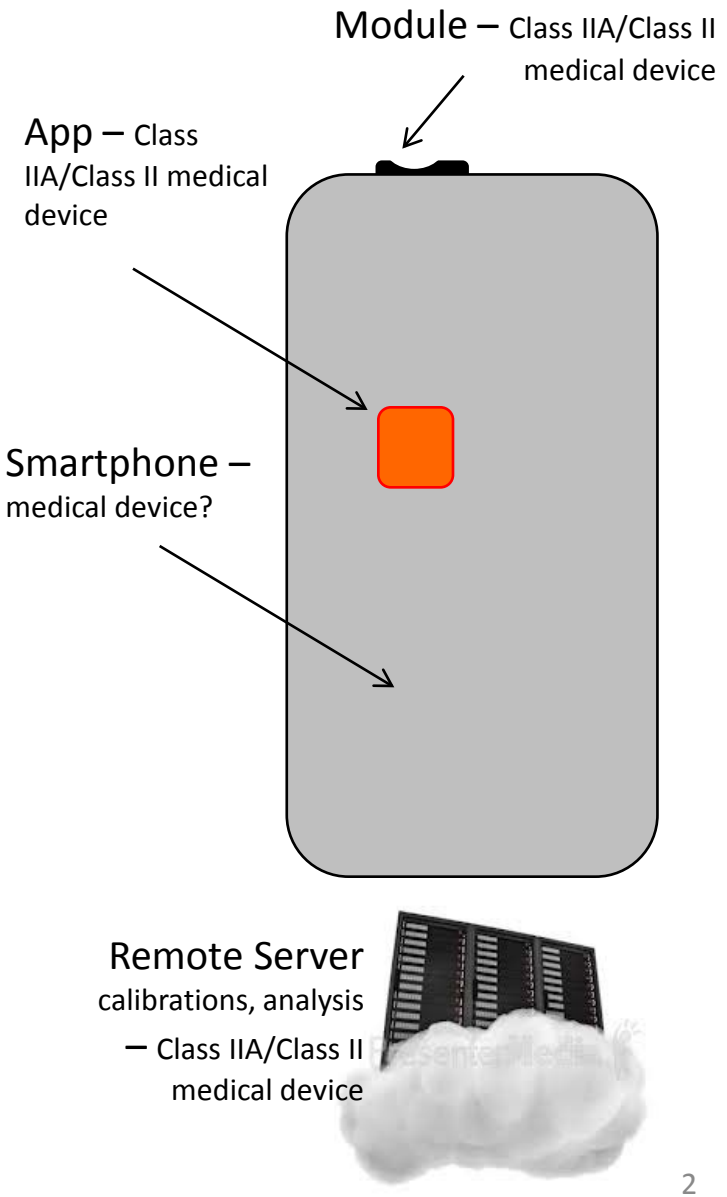
Mobile devices that sense Vital Signs

Case study

Smartphone Vital Signs System:

- Hardware is small enough and cheap enough to incorporate in a smartphone
- SVSS includes everything for medically accurate measurements of all 5 physiological "Vital Signs"
  - Blood pressure
  - Temperature
  - Respiration rate
  - Heart rate
  - Blood oxygen

  and also ECG
- System includes hardware, app and server
- We believe that our package of technological solutions means that the Smartphone is not a medical device



Issues for the app

- Classification
  - Class IIA in Europe
  - Class II in USA
- Safety
  - IEC Class B: Non-serious injury is possible
  - FDA “Moderate”: failure or latent design flaw could directly result in minor injury, including through incorrect or delayed information
- Design and development
  - risk-based
  - good software practice – planned, through life, structured design, traceable (inc SOUP and OS), verified, documented
  - evolutionary development within that framework
- Usability
  - key issue for consumer devices (and Regulators)
- Security
  - confidential health data

Issues for the system including app

- Security
  - how to avoid pirate app (key issue for Regulators)
  - how to deal with rooted ‘phone
- Function
  - Smartphone must deliver as spec through life
    - software upgrades?
    - other apps? (legitimate 3rd party, pirate, interfering)
- Vigilance
  - fundamental requirement of medical device regulation - monitor performance in use and deal with “adverse events” (“arisings” in aerospace language)
  - easier with an internet-connected device and dedicated Remote Server

Some key relevant standards

- Safety
  - IEC60601-3 Section 14 – Programmable Electrical Medical Systems
  - IEC 62304
  - FDA Guidance May 11, 2005
- Usability
  - IEC 62366
  - FDA Guidance June 22, 2011
- Security
  - ISO 27001
  - FDA Guidance June 14, 2013
- Risk Assessment
  - ISO 14971
- Performance
  - ISO81060, ISO 80601-2-61, ISO 80601-2-56/ASTM 1965 ….

All within a QMS framework of ISO13485

Conclusions

- It is possible to develop embedded software to satisfy medical device regulations within a Smartphone environment
- At its heart, it's just good software engineering

but

- Must take account of special circumstances:
  - users are consumers not experts
  - environment must be stable (pirates, hackers, upgrades …)
  - objective evidence is needed to support claims for safety and efficacy to satisfy Regulators before sale

ADELARD

CITY UNIVERSITY LONDON

Health apps: regulation and quality control

A nuclear perspective

Professor Robin E Bloomfield FREng

19th Nov 2014

Exmouth House 3–11 Pine Street London EC1R 0JH
T +44 20 7832 5850 F +44 20 7832 5853 E office@adelard.com W www.adelard.com

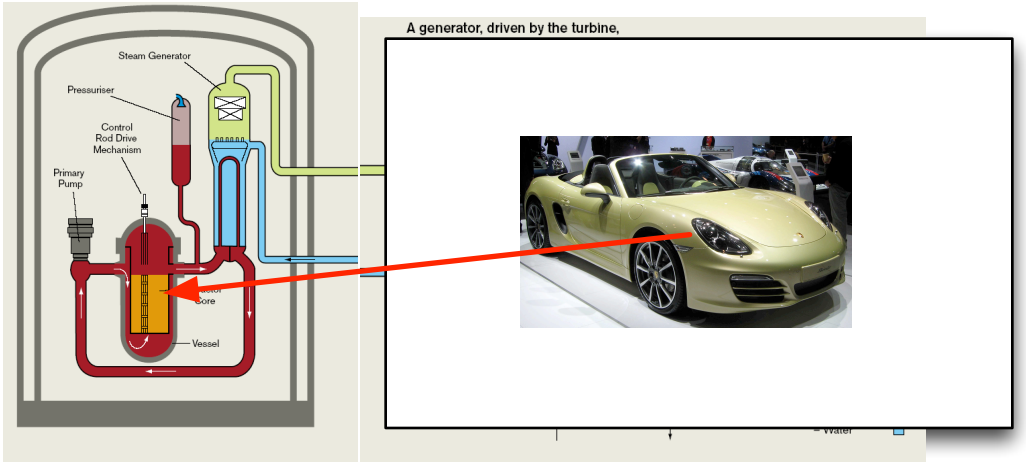
Background

- Trustworthiness of computer based system
  - Safety, security and socio-technical perspective
- Deep and broad experience in nuclear industry
  - Practitioner and researcher; Nusac
- In medical sector
  - Health foundation projects
  - Assessing devices
    - Safety, investment
  - Training manufacturers
  - Research liaison with FDA

Background

- Review of 2005-09 Medical Device Reports (MDRs) found:
  - 56,000 MDRs related to infusion pumps, 710 deaths, 87 recalls
  - Several design problems (e.g. software, user interface) seen as "preventable"
  - FDA concluded that there are "numerous systemic problems with device design, manufacturing, and adverse event reporting"
- FDA decided to **proactively** and **systematically** address **the root causes** of infusion pump recalls

Nuclear power plant

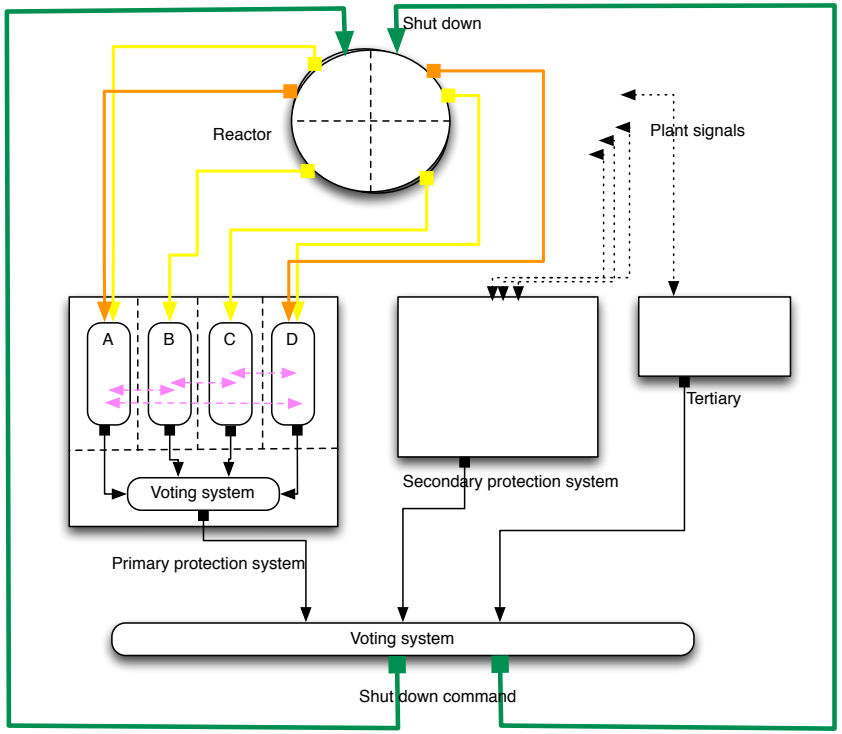


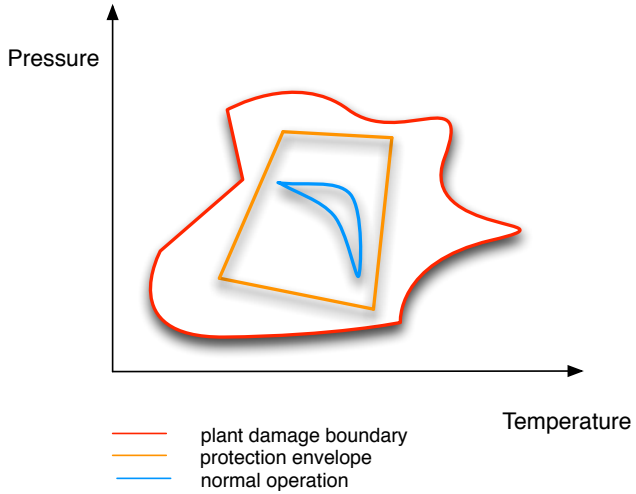
6 times the size of a Porsche 918, 8205 x power

Overview

- How critical are the systems
  - What are safety properties? hazards?
- What is framework for assurance
  - Safety Assessment Principles
  - Claims, Argument Evidence
- What is the approach
  - Understanding
  - Excellence of production
    - Compensation
  - Confidence Building
    - Statistical testing, static analysis

Protection systems





diverse signals

A, B, C, D redundant channels

Primary, Secondary, Tertiary - diverse systems

segregation

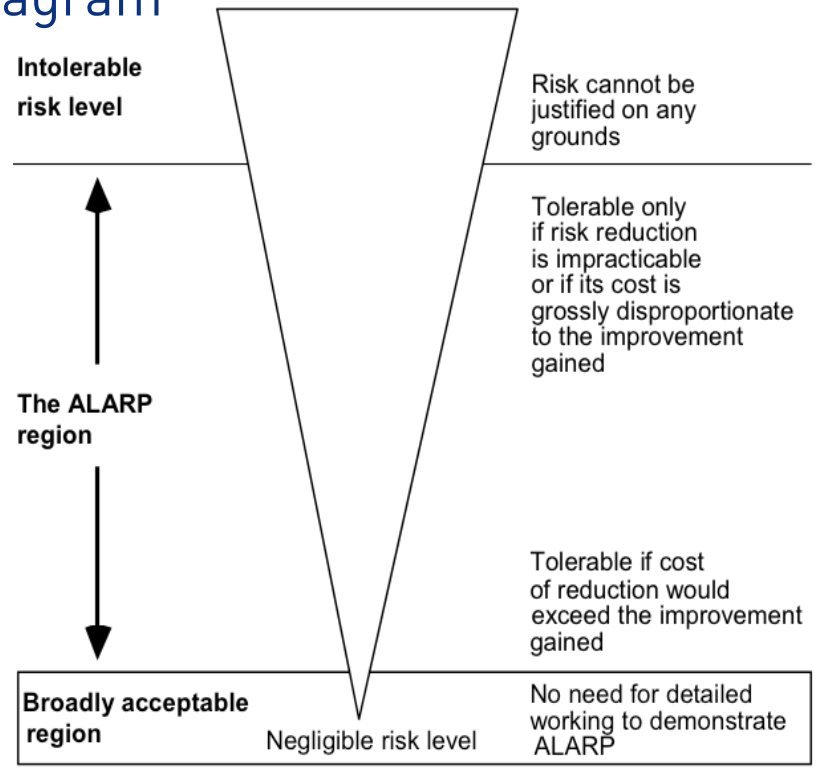
communication between channels

The need for trust in computer-based systems.

Computer systems play a key role in all layers of defence in depth

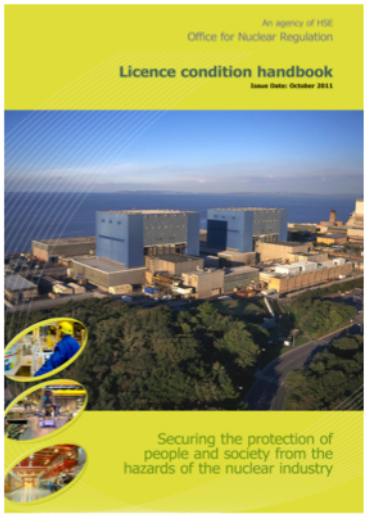
- Normal operation - control, control room information
- Limitation and warning systems
- Trip systems
- Post trip shut down
- Severe accident management

“Carrot” diagram



UK - Safety cases: regulatory obligation

- Safety cases are required by licence conditions.
- The Conditions are *non-prescriptive* and set goals that the *licensee is responsible* for meeting.
- A "safety case" is defined as
  - the document or documents produced by the licensee documentation to justify safety during the design, construction, manufacture, commissioning, operation and decommissioning phases of the installation.
- Safety Assessment Principles (SAPs) describe the safety case process and principles to be covered.

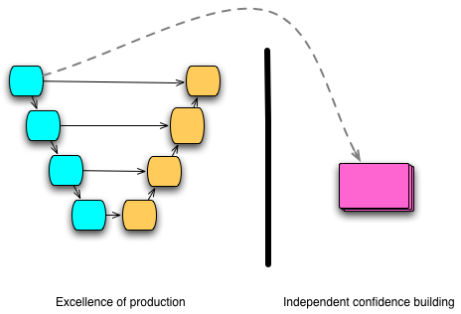


Safety Assessment Principles for Nuclear Facilities - 2006

Fundamental principles	**Safety assessment**	**FP.4**
The dutyholder must demonstrate effective understanding of the hazards and their control for a nuclear site or facility through a comprehensive and systematic process of safety assessment.		

For software – ESS 27

Engineering principles: safety systems	Computer-based safety systems	ESS.27
Where the system reliability is significantly dependent upon the performance of computer software, the establishment of and compliance with appropriate standards and practices throughout the software development life-cycle should be made, commensurate with the level of reliability required, by a demonstration of 'production excellence' and 'confidence-building' measures.		



Summary of principles

1. Effective understanding of the hazards and their control should be demonstrated
2. Intended and unintended behaviour of the technology should be understood
3. Multiple and complex interactions between the technical and human systems to create adverse consequences should be recognised.
4. Active challenge should be part of decision making throughout the organisation.
5. Lessons learned from internal and external sources should be incorporated
6. Justification should be logical, coherent , traceable, accessible, repeatable with a rigour commensurate with the degree of trust required of the system

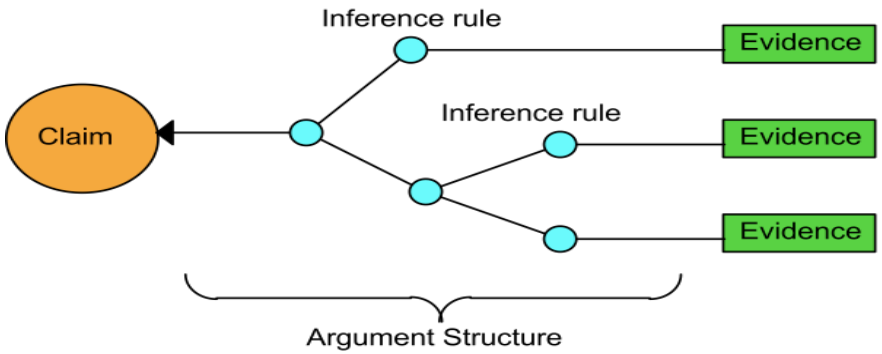
Derived from IAEA, UK Principles – EU Harmonics project

Defence in depth Wenra guidance

DiD level	Associated plant condition categories	Objective	Essential means
Level 1	Normal operation	Prevention of abnormal operation and failures	Conservative design and high quality in construction and operation, control of main plant parameters inside defined limits
Level 2	Anticipated operational occurrences	Control of abnormal operation and failures	Control and limiting systems and other surveillance features
Level 3.a	Postulated single initiating events	Control of accident to limit radiological releases and prevent escalation to core melt conditions	Reactor protection system, safety systems, accident procedures
Level 3.b	Postulated multiple failure events		Additional safety features, accident procedures
Level 4	Postulated core melt accidents (short and long term)	Control of accidents with core melt to limit off-site releases	Complementary safety features to mitigate core melt, Management of accidents with core melt (severe accidents)
Level 5	–	Mitigation of radiological consequences of significant releases of radioactive material	Off-site emergency response Intervention levels

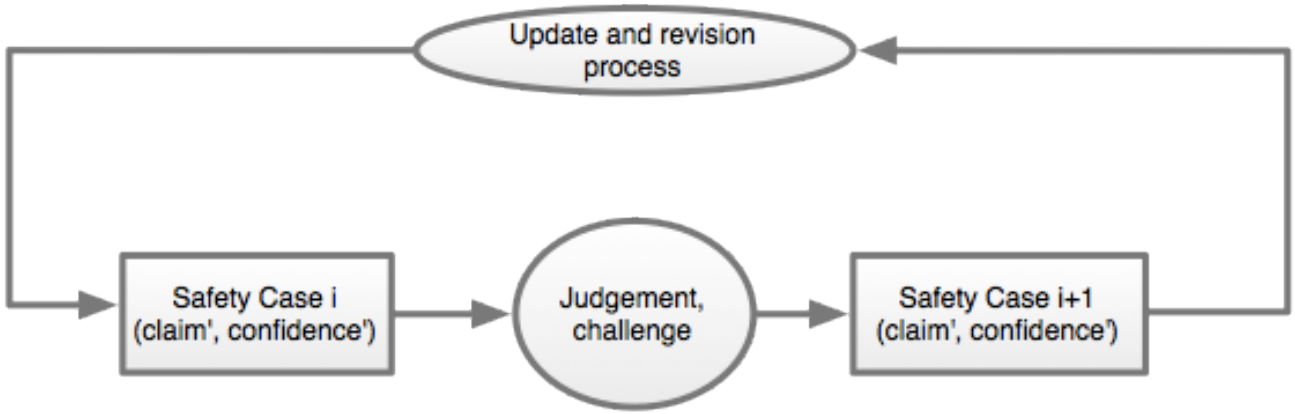
Product-based approaches

- Focus on directly showing the desired behaviour, property or reliability
- They can be applied even when standards compliance cannot be shown
- Linked with specific claims about the product or system
- May use claim-argument-evidence structure

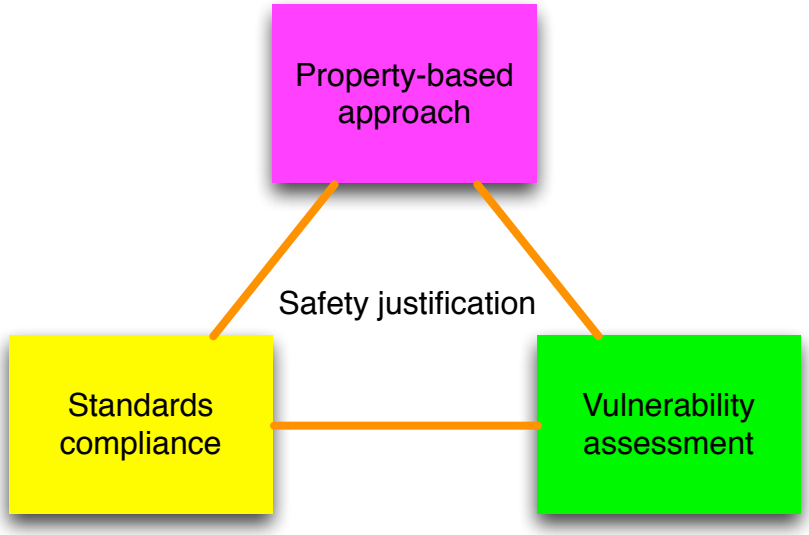


The role of CAE – communication and reasoning

- A method for reasoning about dependability (safety, security, reliability, resilience ...) properties of the system
- Communication is an essential function of the case, from this we can build confidence
  - boundary objects that record the shared understanding between the different stakeholders



Justification approaches – the strategy triangle



Techniques to address properties

PROPERTIES	ANALYSIS TECHNIQUES	TESTING TECHNIQUES
Functionality	Code review / walkthrough Traceability (requirements to code)	Regression testing Statistical testing Black box functional testing Negative testing
Time response	Design inspection Worst-case execution time analysis	Black box functional testing
Accuracy	Numerial analysis	Black box functional testing
Reliability	Analysis of field data	Statistical testing
Robustness		Negative testing Fault injection testing Stress testing
Failure integrity	Failure integrity analysis	Fault injection testing
Operability		Usability testing
Security	Security analysis	Security testing

Techniques to address vulnerabilites

VULNERABILITY	ANALYSIS TECHNIQUES	TESTING TECHNIQUES
Unintended inter-component interaction	Resource usage analysis	Black box functional testing
Incorrect inter-component interaction	Concurrency analysis	Black box functional testing
Application code errors	Coding standards compliance Control/data flow analysis Resource usage analysis Run-time exception analysis Abstract interpretation	Black box functional testing Unit testing Integration testing Random testing / fuzz testing
Unspecified functionality	Traceability (requirements to code)	Random testing / fuzz testing
Errors in embedded components		Black box functional testing

Conclusions

- How critical are the systems
  - What are safety properties? hazards?
- What is framework for assurance
  - Safety Assessment Principles
  - Claims, Argument Evidence
- What is the approach
  - Understanding – hazards, interactions
  - Excellence of production
    - Compensation
  - Confidence Building
    - Statistical testing, static analysis

Medical systems

- Tempo
- Heterogeneous systems
- Patient's own devices
- Accidental systems
- Ad hoc Apps
- Off label
- Local and global
- Multi-stakeholder

Health Foundation Report

Supplement G:

Safety case use within the medical devices industry

Robin Bloomfield, Nick Chozos, George Cleland
Adelard LLP

This is one of a series of supplements to the report: *Using safety cases in industry and healthcare: a pragmatic review of the use of safety cases in safety-critical industries – lessons and prerequisites for their application in healthcare*

To access the report and the other supplements, please visit www.health.org.uk/safetycasesreport

Contents

1 Introduction	G2
2 Medical devices	G2
3 Assurance cases and infusion pumps	G6
4 Other developments	G13
5 Medical device standards	G14
6 Summary	G15
7 Glossary	G16
8 References	G17

ADELARD

CITY UNIVERSITY LONDON

Regulation and Oversight for Developing Automotive Software in Europe

Presented at Academy of Medical Sciences, Nov 2014

Dr Michael Ellims
Sybernetic Ltd.

Surprise!

There is *some*...

Type Approval

Production vehicles can be sold and driven if Type Approved.

Type approval has three parts

- Conformity of production
- Approval of test facilities
- Conformance to regulation

Type approval granted by vehicle certification authority e.g. VCA

Conformity of production

Evidence that a manufacturer can produce something that conforms *every time*.

Quality system – ISO 9001 or equivalent

Control plan

What, why, how, when and who,

Control plans require approval.

Regulation – a lots of it

UNECE (1958 agreement)

- 133 ...to date
- Numerous amendments and corrigendum
- Folded into regulations periodically...

UN GTR (1998 agreement)

- 15 ...to date

Regulation of Software

UNECE 13	Braking, categories M, N and O
UNECE 13-H	Braking, passenger cars
UNECE 79	Steering Equipment
UNGTR 8	Electronic stability control

Note UNECE 13-H also covers ESC !!!

Software Annexes

Special Requirements to be applied to the safety aspects of complex electronic vehicle control systems

UNECE R13	Annex 18
UNECE R13H	Annex 8
UNECE R79	Annex 6
UNGTR 8	clause 132 (almost)

The Annex...

Clause	Regulation Covers	
3.1	Documentation	What is to be presented to certification authority
3.2	Description of functions	A description… all input and sensed data all output boundaries of functional operation
3.3	System layout	Inventory of components Functions of the units Interconnections Signal flow and priorities
3.4	Safety Concept	safe operation under non-fault conditions safe operation under fault conditions Software Safety Analysis
4.1.1	Verification of the system	Under non-fault conditions
4.1.2	Verification of the Safety Concept	Under fault conditions

IEC 61508

Under German law...

- IEC standards are automatically incorporated
  - Implies 61508 should be used for assessing Annexes
- But 61508 doesn't match automotive practice
  - e.g. prototypes not considered
- IEC 61508 "allows" derived standards

So the automotive industry created ISO 26262

...and ISO 26262

Clause	Regulation Covers	Clause	ISO 26262 Covers
3.1	Documentation		
3.2	Description of functions	3: 5.5	Item Definition
3.3	System layout	3: 5.5	Item Definition
3.4	Safety Concept	3: 7.5.2 3: 8.5.1	Safety Goals Functional Safety Concept
3.4.2	Software	-----	Part 6
3.4.4	Analysis (FMEA, FTA etc.)	7.5.1	Hazard analysis
4.1.1	Verification of the system		*missing*
4.1.2	Verification of the Safety Concept	3: 8.5.2	Functional safety concept Verification report

Software 3.1.1 Documentation

(a) The formal documentation package for the approval, containing the material listed in Section 3

(b) Additional material and analysis data of paragraph 3.4.4., which shall be retained by the manufacturer, but *made open for inspection at the time of type approval*.

Software 3.4.2.

In respect of software employed in "The System",

- the outline architecture…,
- the design methods and tools … identified.

The manufacturer shall be prepared, *if required*, to show some evidence of … realisation of the system logic, ...

Weaknesses

Type approval is in general “whole vehicle”

- tests of a vehicle on a test track
- tests as specified in the standard

Formally:

- regulations do not specify deep dives
- certifying authority does not *always* do deep-dives

The Annexes are to some extent “bolt-on”

Some Context...

Data2013 Fortune 500 and World Bank data

Rank	Entity	GDP/Rev	Rank	Enity	GDP/Rev
	Norway	$512 billion	*26*	**Ford Motor**	$147
1	Wal-Mart	$476	*27*	**General Electric**	$146
2	Royal Dutch Shell	$459	*61*	**Nissan Motor**	$104
8	**Volkswagen**	$261	*63*	Tesco	$103
9	**Toyota Motor**	$256	*68*	**BMW Group**	$101
	Portugal	$220	*68*	Électricité de France	$100
13	Samsung Electronics	$208	*90*	Boeing	$ 86
	New Zealand	$185	*103*	Airbus group	$ 78
15	Apple	$170	*155*	**Robert Bosch**	$ 61
20	**Daimler**	$156		**Uruguay**	$ 55
21	General Electric	$156	*181*	Caterpillar	$ 55

Financial Motivation

Minimum recall cost $50 –

Ford Foci per year (approximate) - 1 million

Typical production run - 4-5 years

$50 * 1 million * 5 years

$250 million

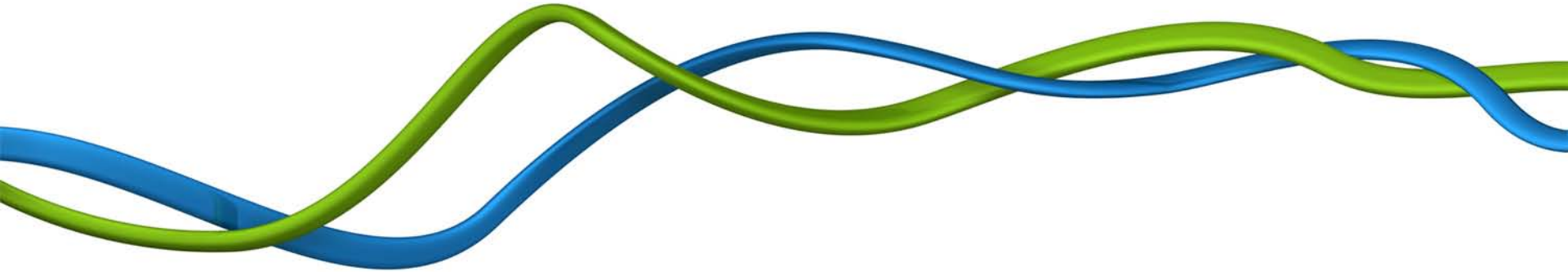
Thank You!

Contact details:

Email: michael.ellims@tesco.net

Mobile: 075 44 68 58 94

ROYAL
ACADEMY OF
ENGINEERING



ROYAL ACADEMY OF ENGINEERING

Software for Dependable Systems – *Sufficient Evidence?*

Martyn Thomas CBE FREng
Non-executive Director, Health and Safety Executive

ROYAL ACADEMY OF ENGINEERING

Summary

Towards certifiably dependable software

The building blocks for a credible *dependability case*

- Explicit Claims
- Evidence
- Expertise

ROYAL ACADEMY OF ENGINEERING

Explicit Claims

No software can be equally dependable in all respects and under all conditions of use.

The dependability case should therefore be explicit about the properties that are being claimed, the assumptions that have been made about the environment, and the level of dependability being claimed.

Different properties may be assured to different levels of dependability

ROYAL ACADEMY OF ENGINEERING

Evidence

Concrete and valid evidence should be provided that substantiates the dependability claims.

Evidence + Assumptions ⇛ Properties *the dependability argument*

Testing is essential, but can *almost never* provide adequate evidence on its own.

Evidence from analysis will be required.

Evidence of the development process is also needed, e.g. to show that the software in use is the same as that analysed and tested.

ROYAL ACADEMY OF ENGINEERING

Expertise

To develop dependable software, engineers need expertise in software development, in the application domain, and in the broader system context.

Software is only part of the system. It must work dependably with other software, hardware *and the users.*

Producing adequate *evidence* is highly demanding and stretches best practice to the limit. Developers must know the best methods and tools and only deviate from them with good reasons (clearly documented).

ROYAL ACADEMY OF ENGINEERING

The full report can be downloaded, free, from

http://sites.nationalacademies.org/cstb/CompletedProjects/CSTB_042247