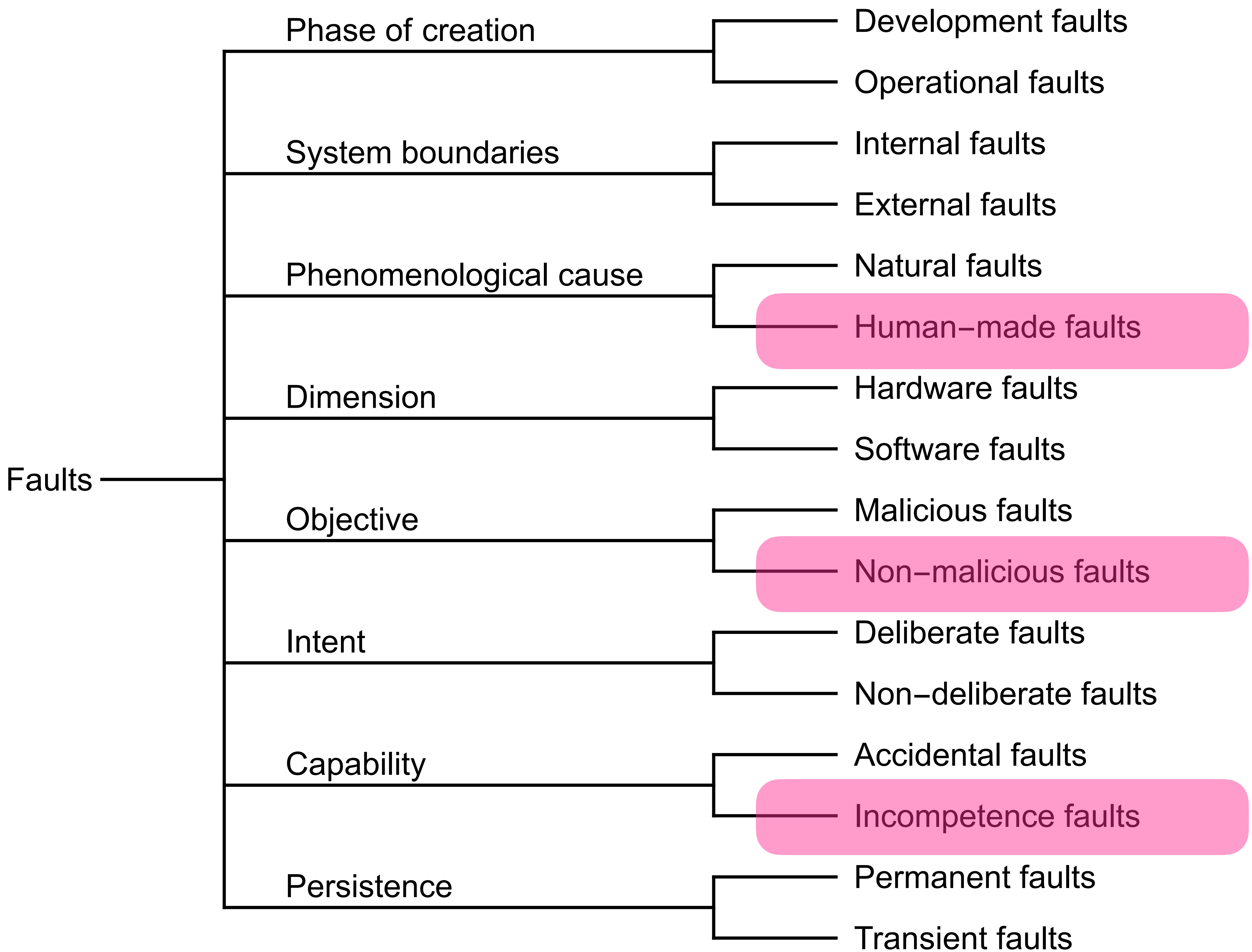
IFIP WG10.4
Human contributions
to dependability and trustworthiness

Harold Thimbleby

What does dependability need?

?


Faults
Phase of creation
Development faults
Operational faults
System boundaries
Internal faults
External faults
Phenomenological cause
Natural faults
Human–made faults
Dimension
Hardware faults
Software faults
Objective
Malicious faults
Non–malicious faults
Intent
Deliberate faults
Non–deliberate faults
Capability
Accidental faults
Incompetence faults
Persistence
Permanent faults
Transient faults

- Modularisation
- Information hiding
- Separation of concerns
- Reduce dependencies
- Invariants & assertions
- Documentation
- Formal methods…

Peter Landin’s problem

…most people don’t understand even simple programs

```
function f(n)
{
  for( var i = 2; i < n; i++ )
     f(i-1);
  print("*");
}
```

Press release

Wrongful Post Office convictions to be quashed through landmark legislation: 13 March 2024

Hundreds of innocent sub-postmasters wrongly convicted as a result of the Horizon scandal will have convictions quashed following landmark legislation introduced today [Wednesday 13 March].

Horizon code

Example

```
If lstockrootnode = 3013 Or lstockrootnode = 3016 Then
     bremedprods = False
     intbalancerootlevel = 5
     lbalancerootenode = 3017
     If lstockrootnode = 2493 Then
         bremedprods = False
         intbalancerootlevel = 3
         lbalancerootenode = 3006
     End If
 Else
     bremedprods = True
     intbalancerootlevel = 5
     lbalancerootenode = 3017
 End If
```

Horizon code

Example

```
bremedprods = lstockrootnode ≠ 3013 & lstockrootnode ≠ 3016
intbalancerootlevel = 5
lbalancerootenode = 3017
```

3 simple lines of code instead of 14
and raises review questions

Horizon code

Example

```
bremedprods = lstockrootnode ≠ 3013 & lstockrootnode ≠ 3016
intbalancerootlevel = 5
lbalancerootenode = 3017
```

3 simple lines of code instead of 14
and raises review questions

Magic numbers

- CS like defining numbers with `zero`, `succ`, `pred`
- What does `3013` mean?
- What does `succ 3013` mean?
- The meanings of magic numbers and their meanings as numbers have dependencies
- They are a bad idea! They undermine dependability

The bad code is (also) a symptom

- The requirements?
- The decision tables?
- The supervision?
- The code review?
- Errors go all the way down (or up)

People don't know ***what*** they don't know

People don’t know ***that*** they don’t know to work within a decade.

Firms hold hacking contests to recruit teenage IT experts

Nicola Woolcock
Education Correspondent

Tech-savvy teenagers are being hired straight from school by companies staging "hack off" competitions.

Bosses are seeking to protect themselves from cyberattacks like the ransomware outbreak that crippled the NHS earlier this month.

At least one organisation has invited job applicants to hack into its own systems to see who can do so fastest.

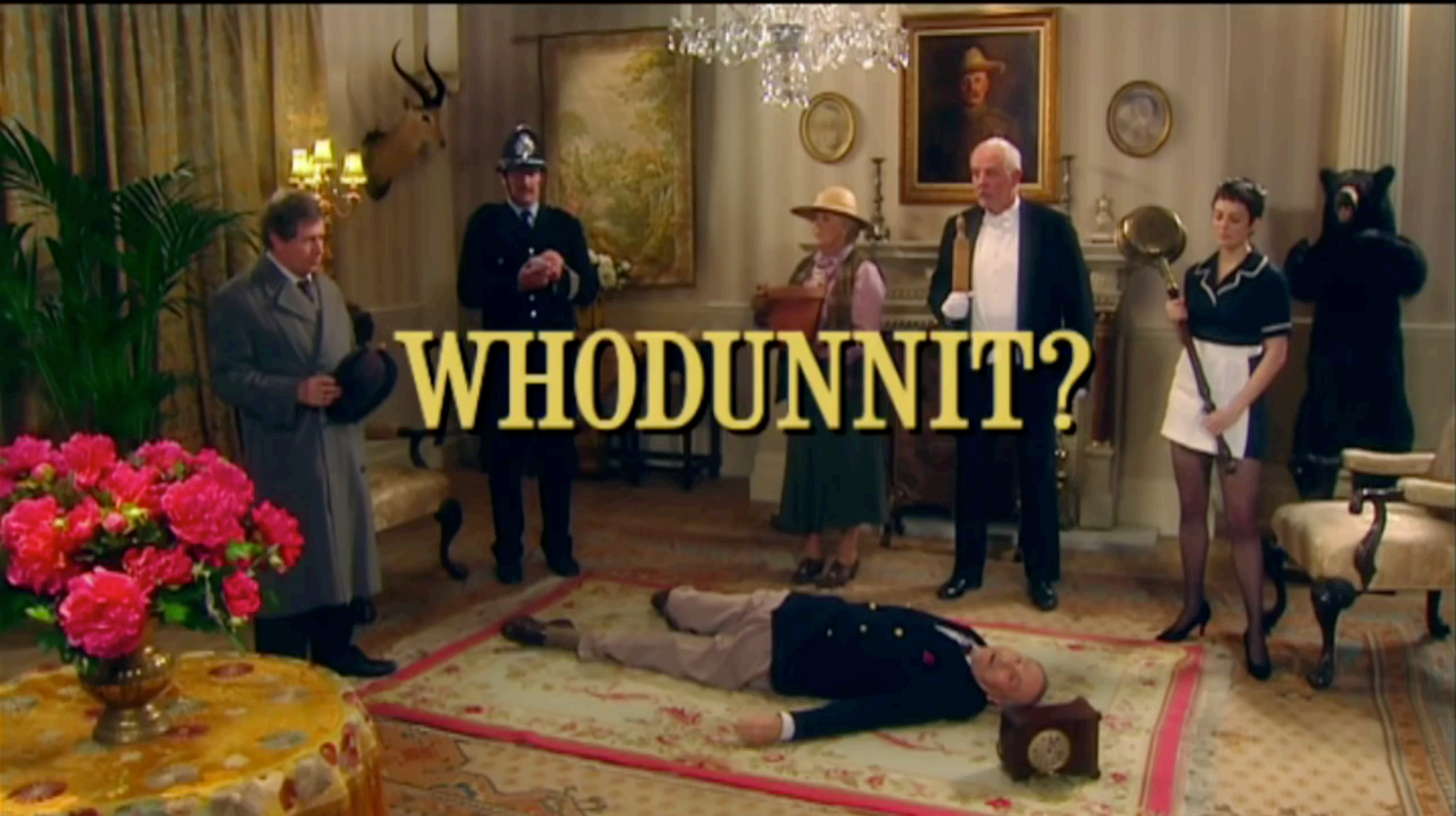
Computer science degrees have previously been criticised for failing to give students the skills they need in the workplace. *The Times* reported in 2014 that computer science graduates learnt

found in retail and restaurants, manufacturing, and financial and business services. Financial services placements increased by 24 per cent.

Ann Swain, chief executive of Apsco, said: "The IT and tech sector is no longer about CVs and qualifications. Businesses are looking for self-taught youngsters who may be fresh out of school, or graduates who have first-hand experience of hacking and cyber-attack.

"Increasingly, teenagers are sought-after — those who have a real passion and talent for IT and can enter at junior level and be organically trained into the corporate world.

"We need to recognise the demand


WHODUNNIT?


WHODUNNIT?



DEFENDER
CU15 XEM

1 July 2014 Last updated at 18:34

Share

Another Princess of Wales Hospital nurse suspended in records inquiry

Abertawe Bro Morgannwg University Health Board confirmed a further seven nurses had been suspended

Another nurse has been suspended as part of an inquiry into the alleged falsification of patient records.

That brings the number of suspensions to 13 at the Princess of Wales Hospital in Bridgend, and one at Swansea's Morriston Hospital.

Abertawe Bro Morgannwg Health Board said it had been carrying out audits and spot checks of blood glucose record-keeping across all its sites.

Three people have been charged by police.

Related Stories

- More record inquiry nurses suspended
- Suspended nurses inquiry 'alarming'
- Nurses suspended in records inquiry

Top Stories

Pressure grows on Russia over crash

- UK demands access to MH17 crash site
- Egyptian troops killed at checkpoint
- UK storms cause further disruption
- Casualties mount in Gaza conflict

Features

Five to watch
Inspiring tales from athletes heading to Glasgow 2014
BBC SPORT

Victorian Strangeness
The era when it was fashionable for ladies to limp

Last survivors
Who will keep Holocaust memories alive?

Dying trade
Are these the last master craftsmen in England?

Little or large
Why cyclists who fly uphill do not have thighs like these

Most Popular

Shared | Read | Video/Audio

Precision XceedPro
Patient ID
02061935
Smith,
John Q
01/23/63 M
Confirm Year of Birth
SCAN
CLEAR
MENU
ENTER
ON/OFF
Xceed = mc²*
*monitoring control
The Precision XceedPro is a highly intelligent monitoring system designed for hospital use. It not only enables testing of multiple patients but also offers TrueMeasure test strip technology to detect adequate sample size and automatic calibration for blood glucose and blood ketone testing. Safeguards such as individually foil-wrapped test strips reduce the risk of test strip contamination.
With features such as TrueID that help positively identify patients by name, gender and date of birth, and TrueAccess that provides lock-out technology to help you ensure compliance with procedures, the Precision XceedPro is set to make other monitoring systems appear relatively ordinary.[1]
Precision XceedPro
Precision Xceed Pro, TrueMeasure, TrueID and TrueAccess (*delete as appropriate) are trademarks of the Abbott Group of Companies in various jurisdictions. 1: Data on file: Abbot Diabetes Care 2011. Date of preparation: March 2011 AXMDP110096
Abbott
A Promise for Life

With features such as TrueID that help positively identify patients by name, gender and date of birth, and TrueAccess that provides lock-out technology to help you ensure compliance with procedures, the Precision XceedPro is set to make other monitoring systems appear relatively ordinary.[1]

Precision
XceedPro

IN THE CROWN COURT AT CARDIFF

REGINA

AND

CLAIRE CAHILL
JADE PUGH

RULING

The distribution of the data very strongly suggests some form of manipulation and suggests that CH20 has lost significant amounts of original data, and **it is not possible to countenance an explanation consistent with the data being reliable**.

Nurses Cleared Of Neglect Allegations

Wednesday, October 14th, 2015 1:00pm

Text editing

- Everyone thinks everyday editing is dependable
- And that dependable editing is correct
- Rather, most people haven’t thought about dependability
- It isn’t very predictable

IFIP WG10.4
Human contributions
to dependability and trustworthiness

Harold Thimbleby

Standard HTML editing

HTML Living Standard textarea
50 columns x 10 rows

```
IFIP WG10.4
Human contributions
to dependability and trustworthiness

Harold Thimbleby
```

Standard HTML | MS Word | Predictable

MS Word editing

MS Word styled textarea
50 columns x 10 rows

```
␣␣IFIP␣WG10.4¶
␣␣Human␣contributions¶
␣␣to␣dependability␣and␣trustworthiness¶
¶
␣␣Harold␣Thimbleby¶
```

Standard HTML | MS Word | Predictable

Predictable editing

Predictable [textarea]
50 columns x 10 rows

```
IFIP WG10.4
Human contributions
to dependability and trustworthiness

Harold Thimbleby
```

Standard HTML | MS Word | Predictable

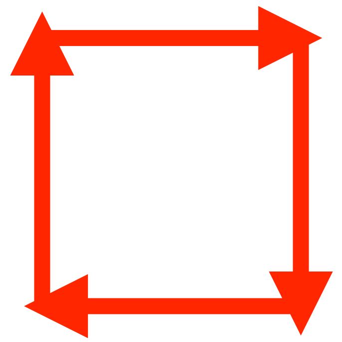
The cursor moves predictably and can go anywhere

Insights… dependability requires modularisation

- MS Word etc do **not** provide dependable editing
- Their code might be dependable,
  but bad user interface design undermines dependability
- Modules hide implementations
- MS Word **exposes** complex editing implementation
- Think of user programming…
- "Predictable editor" – hides implementation, easy to use

User interface theorems

- Euclidian θm: up right down left = I



- In MS Word editing (for sample text)
  Euclidian is true 6.2% of the time

- In predictable editing (as demoed)
  Euclidian is true 88.2% of the time

- Can be reimplemented to be 100%

- And **all** cursor positions are reachable

Obviously you want cars to be dependable for their drivers

Some are

Some aren't


DEFENDER


DEFENDER
CU15 XEM


EV
START
STOP


1:05 PM
Mon, 13/04
Prue
Harold
Guest
Drive safely and obey traffic rules. Watching this screen while the vehicle is in motion can lead to serious accidents.
Make selections only while stopped. Some map data may be incorrect.
Please read the safety instructions in the Navigation Manual.
Confirm
Language

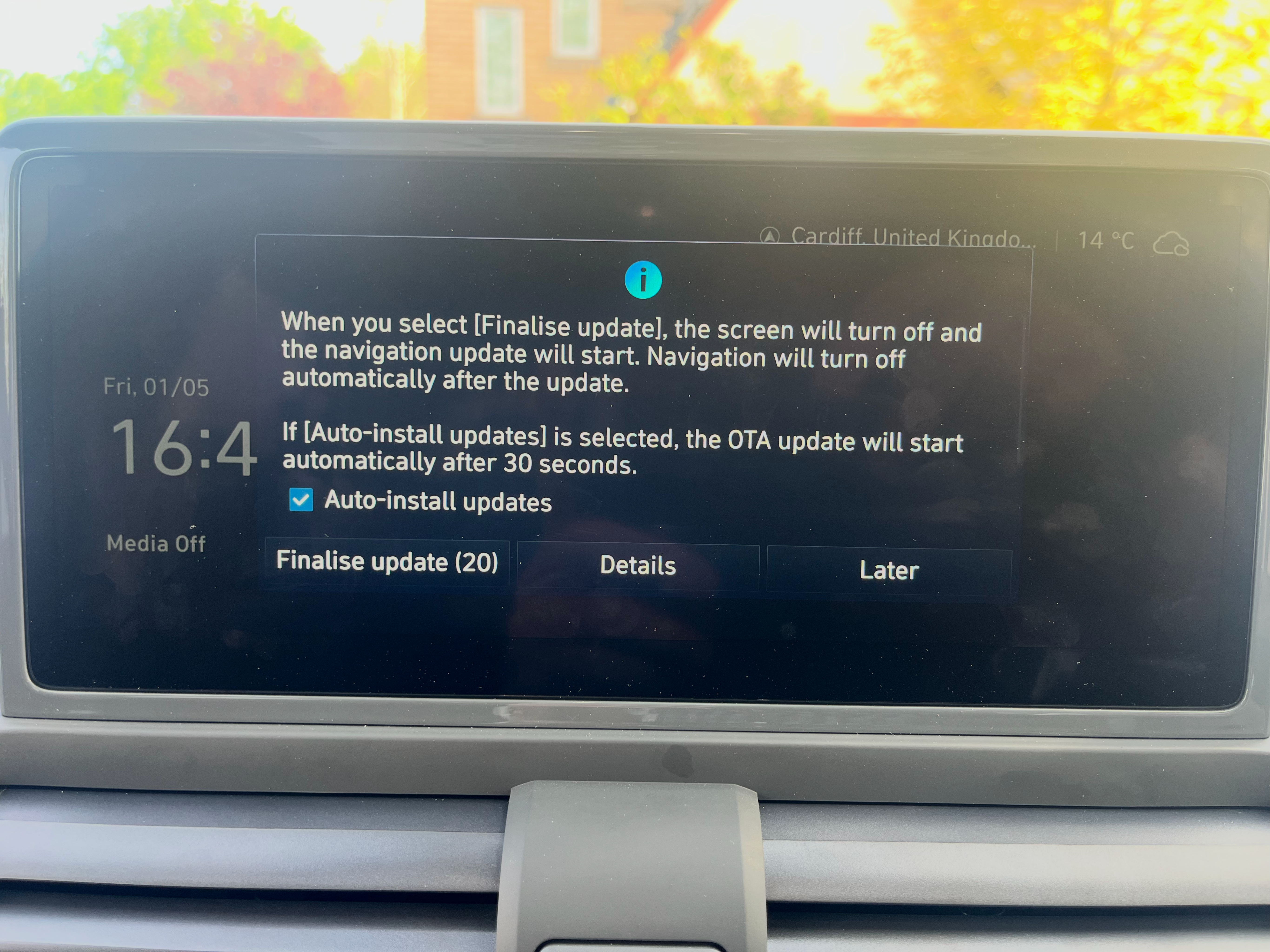

What's new
1:13
For more information on the infotainment system update, press [Details].
Details
Close

What’s new

For more information on the system update press Details.

Details

Close


Cardiff, United Kingdo...
14 °C
Fri, 01/05
16:4
Media Off
When you select [Finalise update], the screen will turn off and the navigation update will start. Navigation will turn off automatically after the update.
If [Auto-install updates] is selected, the OTA update will start automatically after 30 seconds.
Auto-install updates
Finalise update (20)
Details
Later

Hyundai developers …

- Don’t read their own specifications!
- a) Watching the screen can lead to dangerous accidents
- b) Please look at the screen!
- Other examples: **the car is not predictable**
- Therefore the car is **not dependable for drivers**


Recuperation conditions not met
Cardiff, United Kingdo... | 9°C
AUTO
OK

60
40
80
20
100
120
MPH
88 %
D
20
Range guide
206 mi
Min
134mi
Max
244mi
CHARGE
POWER
READY
18℃
280 mi

D
20
Range guide
206 mi
Min
134mi
Max
244mi
60
40
80
20
100
0
120
MPH
88 %
READY
18℃
CHARGE
POWER
STOP
280 mi

D
40
8.8mi
i-PEDAL
Range guide
EV battery charge
too low to display
the range.
60
40
80
20
100
0
120
MPH
0
1
19 %
READY
13℃
35mi
CHARGE
POWER
Level
399 mi

The point is…

- Most code grows
- Most code is as good as incomprehensible
- It might be dependable in some sense
- But it is not dependable **for use**

CrowdStrike worldwide failures

- 19 July 2024 — faulty software update
- 8.5 million PCs worldwide crashed
- Caused by CrowdStrike's own "Falcon" software
-

> [...] **THE SOFTWARE AND ALL OTHER CROWDSTRIKE OFFERINGS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND** [...] **TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW CROWDSTRIKE SHALL NOT BE LIABLE** [...]

The point of CrowdStrike

- To make systems more dependable
- Yet it isn't dependable itself!

If manufacturers won’t provide a
warranty that their software is dependable
then it is not dependable

Summary

- The culture (eg warranties) is software is not dependable
- But it is treated as dependable
- There is no certification that developers are competent
- But they are treated as competent
- Many people developing don’t even realise it
- AI makes it worse

Conclusions

- Dependable systems must be dependable **IN USE**
- We have to take developers' **unconscious incompetence** into account
- Including our own
- We have to fight popular culture:
  - We need legislation to improve
  - We need more theory


OXFORD
Fix IT
How to see and solve the problems of digital healthcare
FRESENIUS MEDICAL CARE
10 L
Filtrate bag
HAROLD THIMBLEBY

Airway management; Anesthesia for neurosurgery; Anatomy; Basic sciences to underpin anesthetic practice; Cardiothoracic anesthesia and cardiothoracic critical care; Core anesthesia; Critical incidents; Day surgery; ENT, maxillo-facial and dental surgery; General duties; General, urological, and gynecological surgery; Induction of general anesthesia; Infection control; Intensive care medicine; Intraoperative care; Management of cardiac arrest in adults and children; Management of respiratory and cardiac arrest; Neuroradiology and neurocritical care; Non-operating room obstetrics; Non-operating room orthopedic surgery; Obstetrics; Orthopedic perioperative medicine; Orthopedic surgery; Pediatrics, including child protection; Pain medicine; Perioperative management of emergency patients; Perioperative medicine; Pharmacology; Physics and clinical measurement; Physiology and biochemistry; Postoperative and recovery room care; Premedication; Preoperative assessment; Regional sedation; Statistical methods; Transfer medicine; Trauma and stabilization; Vascular surgery.

Figure 24.1. A selection of the many essential topics a UK anæsthetist must be examined on and pass to qualify so that they can use anesthetic machines built by unqualified developers — compare with figure 24.2.

anæsthetist. If anything goes wrong for an anæsthetist (or anesthesiologist), they might harm or perhaps kill one or two patients.

In complete contrast, if you want to build or program a device that delivers drugs into a patient, you can start making and programming an infusion pump or any other machine *immediately*. No qualifications whatsoever are needed (figure 24.2), whether you are a programmer or other engineer, and there are no requirements to undertake professional development, and no requirements to be certified in any way. You
risk of disqualification.

It's worth pointing out t
do have lots of tim
products are
right

Figure 24.2. All of the topics a programmer must be examined on and must pass to qualify so that they can design and program healthcare systems, such as anesthetic machines — compare with figure 24.1.

so simple they weren't even connect
scale of what Robin Seggelm
ital systems — it aff
scale of the He
tals would
them

https://
www.harold.thimbleby.net/
booklet

Deaths and illness around childbirth had always been a fact of life until 1847, when Dr Ignaz Semmelweis noticed that his hospital wards had a higher rate than the nearby convent hospital. He set out to find out why. What was he doing wrong?

Semmelweis started collecting statistics. He noticed that his wards had fewer sick patients in the summer. But why? He realised that in winter his doctors attended autopsies to learn about anatomy, then went straight back to the wards. In summer they didn't do this so often.

Semmelweis speculated something was getting back to the wards from diseased bodies in the morgue. He instituted hand washing. His intervention soon reduced maternal death from around 20% to 2%.

Unfortunately, Semmelweis met a lot of resistance to his ideas. Doctors didn't like being told they might be the cause of illness. After all, Semmelweis had no real theory why his ideas worked.

A real explanation had to wait until Louis Pasteur developed germ theory, which at first only explained fermentation. The Scottish surgeon Joseph Lister then connected germ theory to putrefaction and disease. Lister realised that antiseptics would destroy germs causing disease, and his success as a surgeon soon became famous. Healthcare was persuaded.

Antiseptics prevent but don't cure disease. Effective cures had to wait for antibiotics, which Alexander Fleming discovered when he identified penicillin in 1928.

Antibiotics are now widely used to treat infections. But in turn, using antibiotics is creating new problems in this invisible world of bugs. Bacteria evolve, and become resistant to antibiotics. Some antibiotics are thus losing their power, which can be catastrophic for infected patients — it's a new global health threat. Guidelines are being developed so antibiotics are only used when they are effective and don't increase antibiotic resistance.

Bugs that cause disease are invisible, and for thousands of years, people could only speculate about illness. Most people just accepted disease.

Eventually, Ignaz Semmelweis worked out a cause of disease, but he met considerable resistance from his colleagues.

Digital healthcare is a new intervention, affecting all areas of healthcare. Digital health has hidden bugs.

Managing digital bugs doesn't require antiseptic procedures, it requires computational thinking. Unfortunately, just like theories of infection in the nineteenth century, computational thinking meets resistance.

Like Semmelweis's colleagues, we resist being told we may be wrong. Moreover, as cat thinking shows, the excitement about digital itself makes it much harder to think about its limitations and weaknesses. Why would we have bought that expensive AI system if it wasn't going to be an effective system?

Just like early ignorance of bacteria, antiseptics, and antibiotics meant that curing disease was almost impossible, ignorance of computational thinking makes it almost impossible to recognise, talk about, or to address the problems of digital bugs.

?

What does **computational thinking** mean?

We haven't defined computational thinking in this booklet. We haven't defined antibiotic either.

You take for granted that to understand antibiotics you need some medical training. It's the same with computational thinking: to understand computational thinking you need computer science and software engineering training.

Chapter 13 in *Fix IT* is all about computational thinking.

There are parallels between antibiotic resistance and digital failure.

Just like the discovery of antibiotics was revolutionary, and antibiotics were first seen as a "magic cure," so, too, people promote digital as a cure-all solution to many of today's healthcare problems. But it's counter-productive to try to solve problems by getting more or newer digital systems — digital transformation — without stopping to ask: Will it be better? Will it be safe and effective? When is enough enough? We won't know unless we understand the underlying computer science.

Think! Computational thinking is the right approach to understand digital.

Dr Semmelweis's students washing their hands in his ward *Fix IT* page 15

Medical device and system manufacturers often complain about regulatory burden — the cost to them of complying with even the current regulations around digital healthcare.

I remember a manufacturer saying that if they followed regulations to the letter, their innovative systems would be so delayed they'd be obsolete by the time they reached the market. I wondered, if things are going to get obsolete so quickly, why would anybody want to spend any money on them?

We wouldn't generally go along with such arguments for drugs — we'd first want to know drugs are safe and mostly free of side effects before they are marketed.

Pharmaceutical companies rarely complain about regulatory burden. They employ highly qualified chemists, often post doctoral, and microbiologists to develop and test new drugs. They take regulation in their stride.

Inexperienced developers use what's called a "happy path" to test their systems. They simply check that things work as they are supposed to work. They can now tell everyone that it works exactly as it's supposed to work — implying any problems are your fault. But the happy path means they didn't check for possible failures.

Competent developers instead test all possible paths where their systems are and aren't used as they are supposed to be. This is very hard, as there are an overwhelming exponential number of ways of using things in unexpected ways. Developers who want to do thorough testing therefore use sophisticated computer tools.

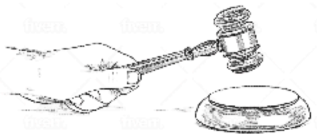
AI, of course, makes safe development **very** much harder — so at least carefully check contracts to ensure manufacturers don't deflect responsibility for safety.

In response to the serious problems of quack doctors, the UK Medical Act of 1858 requires doctors to be formally registered to practice. Similarly, after deaths from accidental poisonings, the Pharmacy Act of 1868, requires drugs to be appropriately labelled, requires keeping written records, and restricts the sale of drugs to qualified pharmacists.

So, when we read about digital health failures in this booklet, why don't we see the bad digital systems as likely developed by "quacks" and "adulterated" with bugs? Digital has become so fundamental to all healthcare, it's time for it to be regulated in much the same way as pharmacy is.

Think! We should accept regulating digital — systems, developers, and support — just like we accept healthcare regulation.

CHECKLIST FOR WHEN THINGS GO WRONG



If you end up in a disciplinary hearing, or in litigation, here's what you should consider . . .

1. You are not alone. Talk to people. Try to find out if other people have had similar experiences — if so, suspect the system, not the people.
2. Check out the NHS Just Culture — for example, it says "Are there indications that other individuals from the same peer group, with comparable experience and qualifications, would behave in the same way in similar circumstances?" — if so, this would be a likely sign of digital problems! (See further reading.)
3. It is important to talk to a competent expert. Although Expert Witnesses are available for court work, a good place to start is to get in contact with your local university Computer Science Department, and talk to someone — maybe a PhD student or Research Assistant — who is working in usability, safety, cybersecurity, or dependability.
4. The freely accessible database *MAUDE – Manufacturer and User Facility Device Experience* has details of millions of medical device issues, and may be relevant to your situation. Search online for "FDA Maude."
5. Require the disciplinary panel or your prosecutors to provide the documents listed below. Where these items won't or can't be provided, everyone should treat evidence with appropriate caution. Your friendly expert (see point 3 above) may need to modify or extend this list, depending on your circumstances.

   Note that in a court case, a judge can order disclosure of facts to an Expert Witness if the organisation is not prepared to provide the documents or access to the systems to determine the facts yourselves.

   (a) A copy of the actual computer-readable evidence (not a paper printout) that they are relying on — so you or experts can analyse it. It must be examined by experts before anyone agrees that the system has produced correct output, and what its significance is.

   (b) Copies of independent certification to the relevant international standards that the digital systems are reliable, and adequate for evidential purposes.

   (c) Evidence of the relevant serial numbers and software version numbers. Without knowing these, it is impossible to confirm how the device(s) will have behaved. It's also possible that old or obsolete software version numbers will indicate that the systems have not been properly maintained.

   (d) Evidence that the systems are suitable for the clinical purposes for which they are used. If they cannot provide this evidence, then they cannot logically rely on any presumption that the electronic evidence they are using is reliable, Common Law presumptions or otherwise.

   (e) Proportionate evidence of the forensic standards followed, to ensure the integrity of the evidence before and during the investigation. Has the device been used since, or reset? Were there system failures or cyberattacks? Does the data include timestamps? Note, for example, with spreadsheet and simple database data, rows and columns may be edited, duplicated, or deleted without leaving any record of tampering or accidental edits.

   (f) Independent confirmation that the data in fact refers to you or your actions. For instance, in many environments, for historical reasons, there may be multiple staff cards in circulation with your ID on them — so "your" ID may not refer to you.

   (g) The contracts with the digital system suppliers. Contracts often impose unnecessary confidentiality, say that clinical outcomes are a result of your professional judgement, and sometimes even require you to indemnify the manufacturers!

FIX IT PRIZE

This booklet is based on Harold Thimbleby's book *Fix IT*, which won the British Medical Association's General Medicine book award. The judging panel said:

"*Fix IT* is such an important book. Our ability to help patients is so reliant on IT and digital solutions. It has the broadest appeal and has achieved something quite impressive. It is not just medically-focused in presenting solutions. A real strength is that it takes examples from outside of healthcare and translates them into healthcare. It should be read by all healthcare staff.

Harold Thimbleby, *Fix IT: See and Solve the Problems of Digital Healthcare*, Oxford University Press, 2021.

The Fix IT prize

In collaboration with the Royal College of Physicians, we have launched an annual prize for digital innovation, **The Fix IT in Healthcare Prize**. The prize rewards excellent innovations in digital healthcare, which help solve the problems described in this booklet, particularly digital initiatives that have improved, or promise to improve, patient safety and staff well-being within the NHS or healthcare internationally.

More details are available from the Royal College of Physicians web site, www.rcplondon.ac.uk, under Funding & Awards.

https://
www.harold.thimbleby.net/
booklet