Building Trust in an IoT Enabled World

Professor Jeremy Watson CBE FREng
IET President
Vice-dean Engineering Sciences, UCL
Chief Scientist & Engineer, BRE

14 September 2017

The Institution of Engineering and Technology

UK General Election 2017 Campaign

The IET is calling on the new Government to back the big engineering issues

MAKE CYBER SECURITY A PRIORITY

The vulnerability of critical infrastructure to cyberattack means organisations must be trained and ready.

Find out more at: www.theiet.org/election2017

Setting the Scene

- Cyber attacks cost businesses as much as $400 billion a year [Lloyds London]
- 99.9% of identified vulnerabilities were exploited within a year after the vulnerability was published [Verizon 2017 Data Breach Investigations Report]
- By 2020 there will be 22 billion connected things [Cisco]
- Interdisciplinary thinking is central to Cyber Security
- Do we need a registration scheme for Cybersecurity professionals?

The Internet of Things (IoT)

- Very broad definition, links to Big Data and Data Analytics
- Smart technologies make previously unintelligent things (like home thermostats, white goods, or building management systems) able to compute and communicate – typically wirelessly
- Almost all the data that IoT devices send is to other machines – there are no humans involved: ‘M2M’ communications
- By 2020, industry experts predict the number of IoT devices to exceed 25 billion (Gartner)
- The possibility of hacking into IoT networks (by humans or machine agents) brings new cyber-threats; i.e. New crime and security issues

Reference - The Internet of Things: making the most of the second digital revolution
The Government Office for Science 2014

Applications of IoT – diverse and pervasive

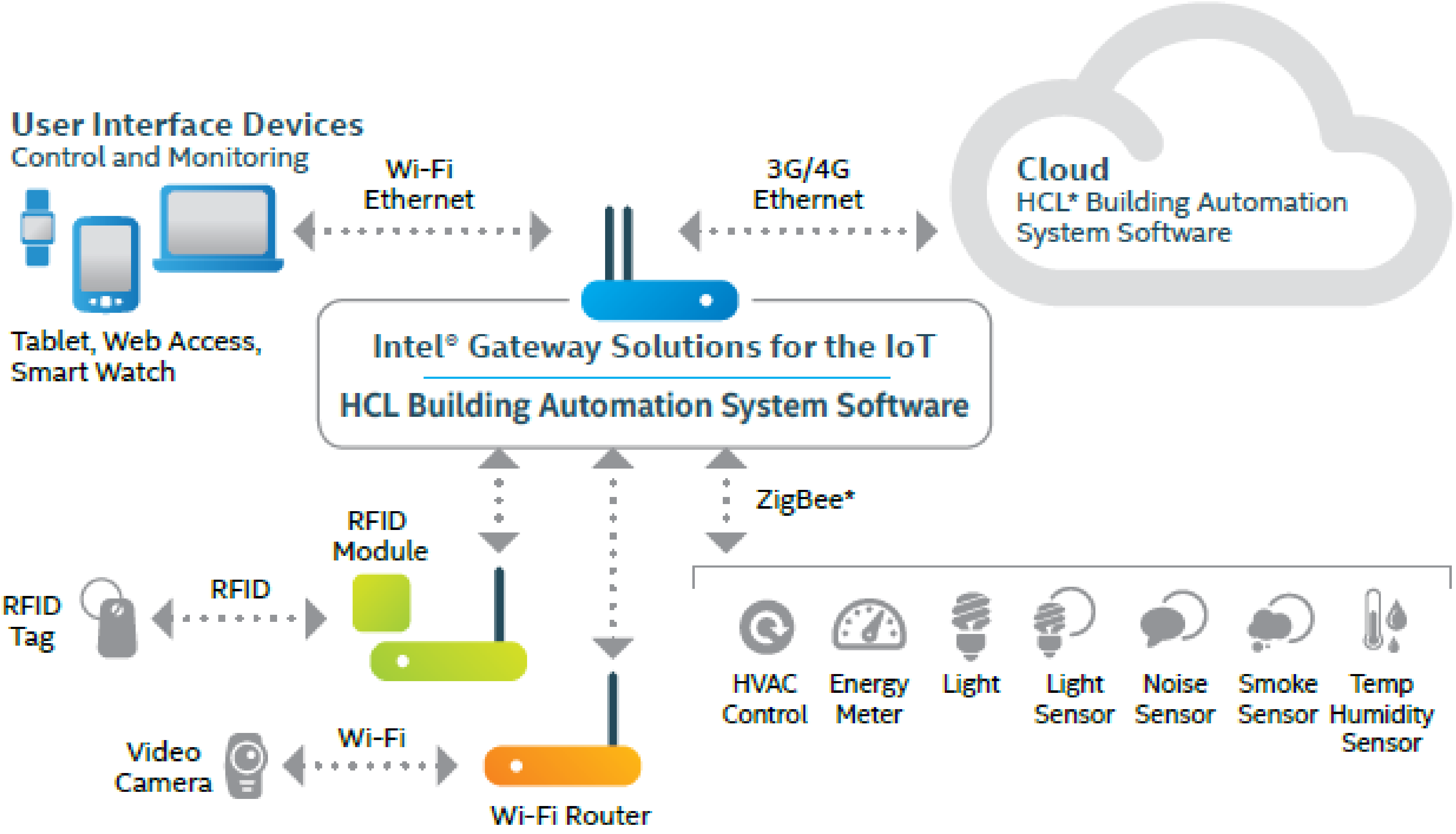
- Households
  - Smart thermostats
  - White goods
  - Televisions
- Building Management Systems (BMS) – sensors and controls
  - Heating, ventilation & air conditioning
  - Access controls
- Industrial and Utilities control systems
  - Sensors and actuators (pumps, heaters, valves, etc.)
- Medical and Hospital equipment
  - Patient monitors
  - Patient information recording
- Transport
  - Condition monitoring
  - Asset location
- Retail

Types of IoT device communication

- Wireless
  - WiFi – to routers
  - Local wireless networks – like LoRa, Zigbee, Bluetooth
  - G3 and G4 (and beyond) – mobile (e.g. Smart Meters)
  - Near-field Communications – NFC (‘Paywave’ or ‘Contactless’) – short range
- Wired
  - Direct IEC 802 LAN connection
  - USB – local devices

The common features are embedded intelligence and ‘Machine-to-Machine’ communication, without human sight or intervention

Applications of IoT - Buildings

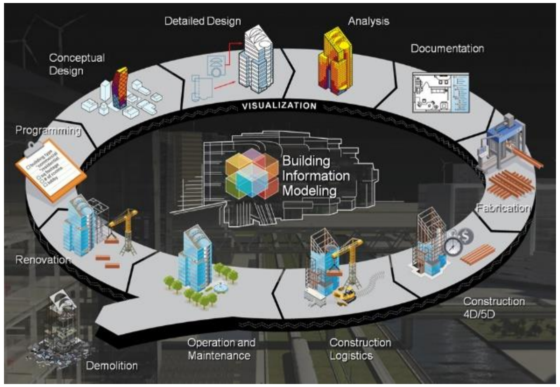


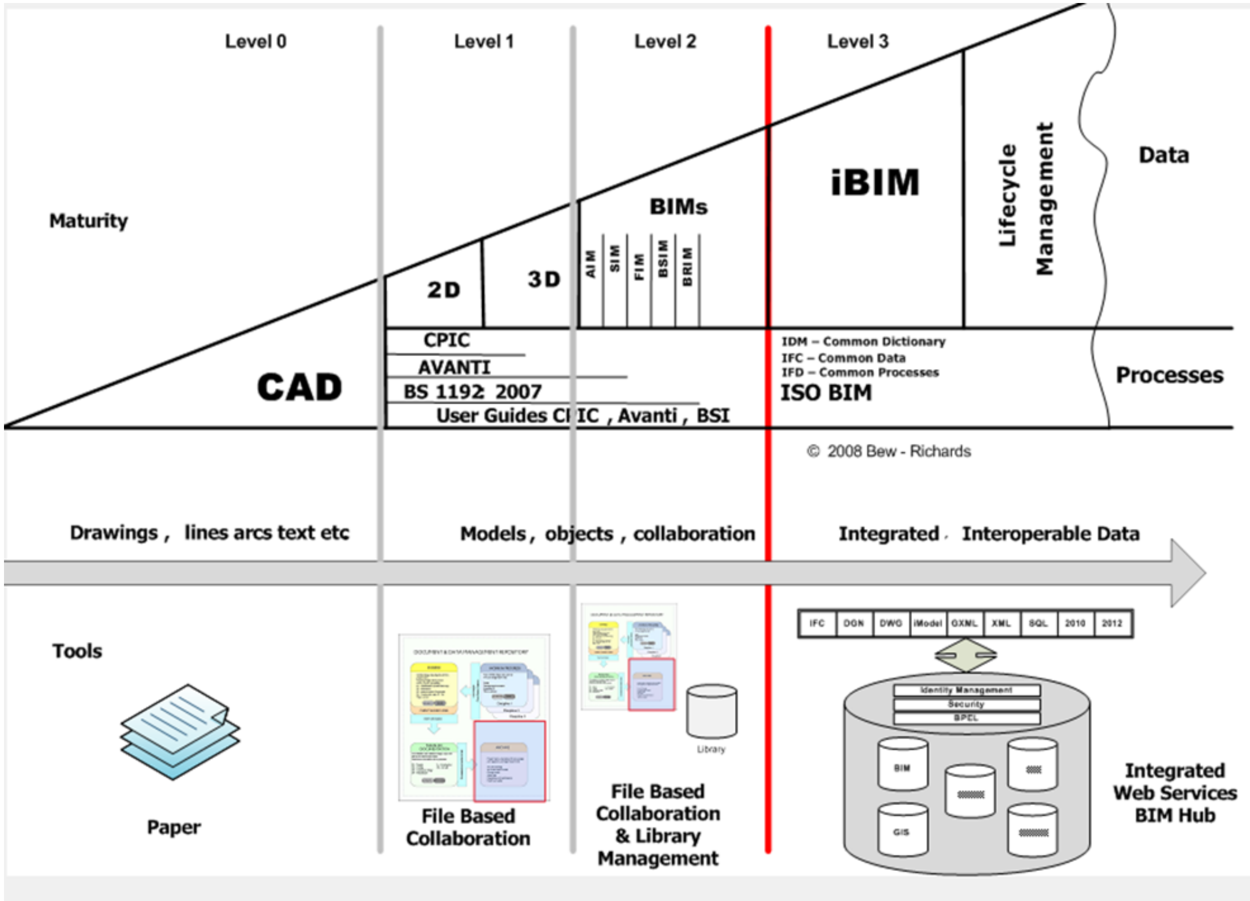
Building Information Modelling

CAD++

BIM Evolution

On a journey from CAD to a responsive, integrated, digital built environment

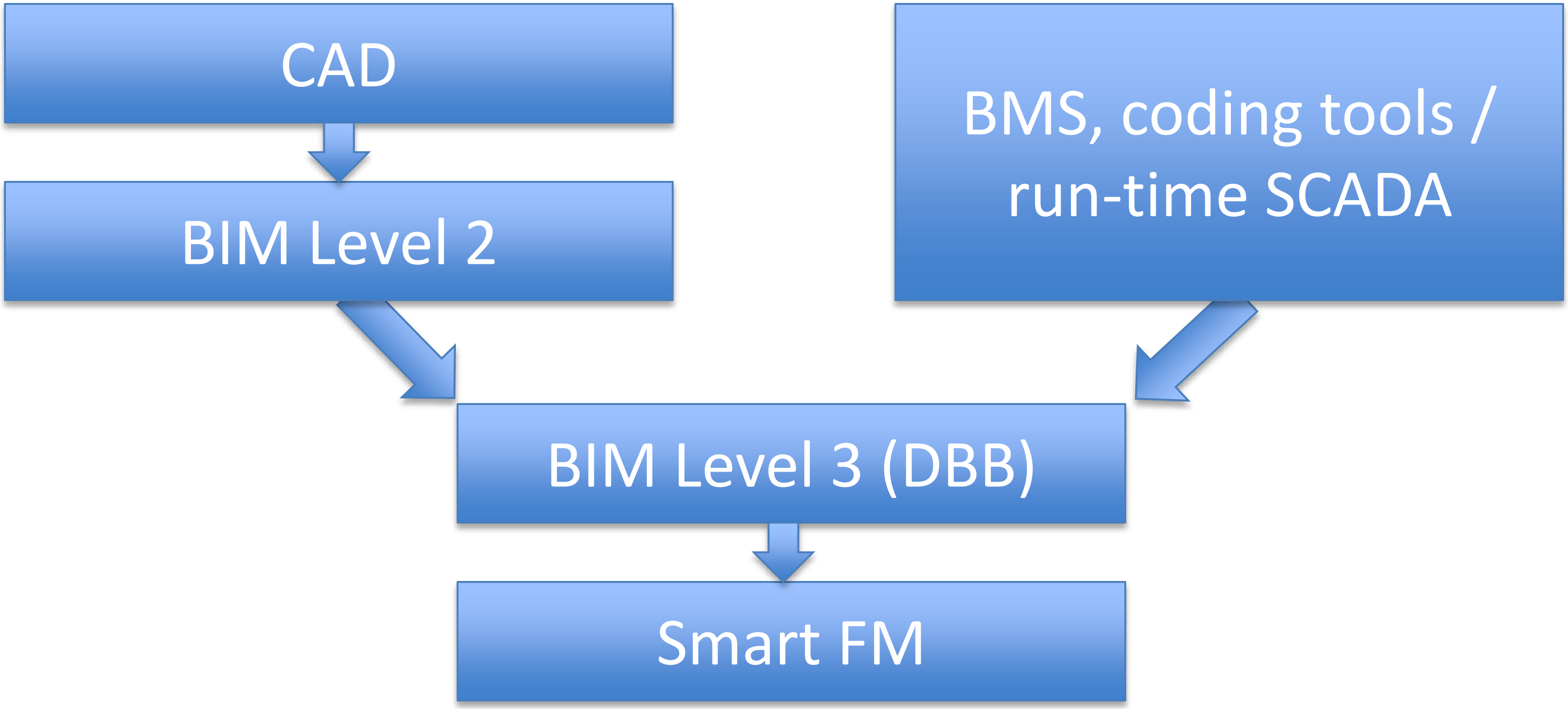




Converging systems view

Building design

Building operation



CAD

BIM Level 2

BMS, coding tools / run-time SCADA

BIM Level 3 (DBB)

Smart FM

Integrated design and operation tools

Digital Built Britain: Facets of BIM Level 3

Static data schema combined with **dynamic values** physically associated with object models i.e. Real-time operational data will be integrated with static design information

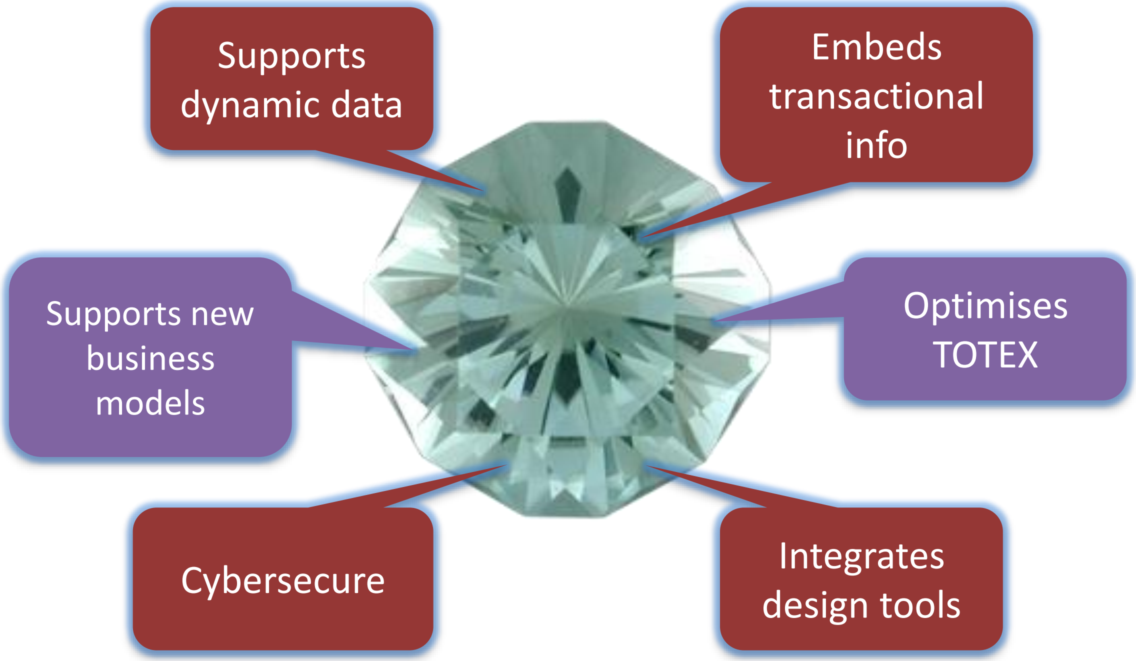
DBB will support **third-party real-time analytics and dashboards**

Actuators will be supported with secure key access

Open data approach to design and run-time tools and data-sharing

DBB must be a high performance, **cyber-secure** schema/system – Secure by design

Is likely to use IoT for measurement and actuation



Supports dynamic data

Embeds transactional info

Supports new business models

Optimises TOTEX

Cybersecure

Integrates design tools

http://digital-built britain.com/DigitalBuiltBritainLevel3BuildingInformationModellingStrategicPlan.pdf

Cybersecurity of IoT in the Built Environment is Vital

- Information theft
  - Personal data, eavesdropping
  - Building occupancy and utilisation (space and time patterns)
- Perturbation of operation
  - Hacking into control networks to perturb asset operation (e.g. denial of a physical service, like aircon for server rooms)
- Corruption and falsification of sensor data
  - Energy theft by hacking smart meters
  - Spoofing BMS
- Falsification of information
  - Supply chain issues
  - Product provenance issues (e.g. pharmaceuticals, aerospace spares)

Blackett Review

Convened by Government Chief Scientific Advisor

- Investigations into matters of national importance (security, economy, etc.)
- Panel of experts plus support from GO-Science and other government departments
- Evolution of recommendations, Report

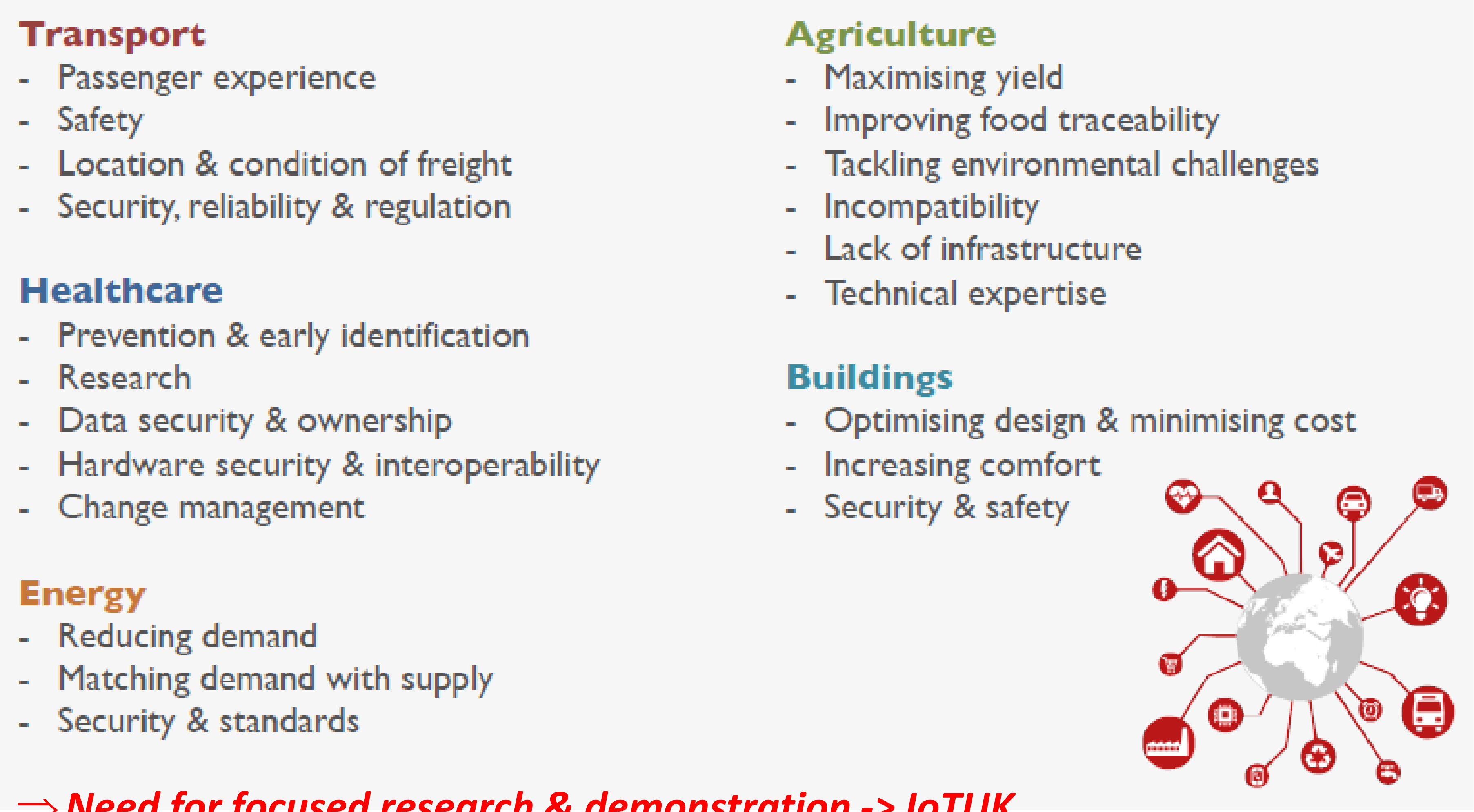
The Internet of Things:

Making the most of the Second Digital Revolution

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/409774/14-1230-internet-of-things-review.pdf

⇒ ***Need for focused research & demonstration -> IoTUK***

Blackett Review: IoT themes



Transport
- Passenger experience
- Safety
- Location & condition of freight
- Security, reliability & regulation

Healthcare
- Prevention & early identification
- Research
- Data security & ownership
- Hardware security & interoperability
- Change management

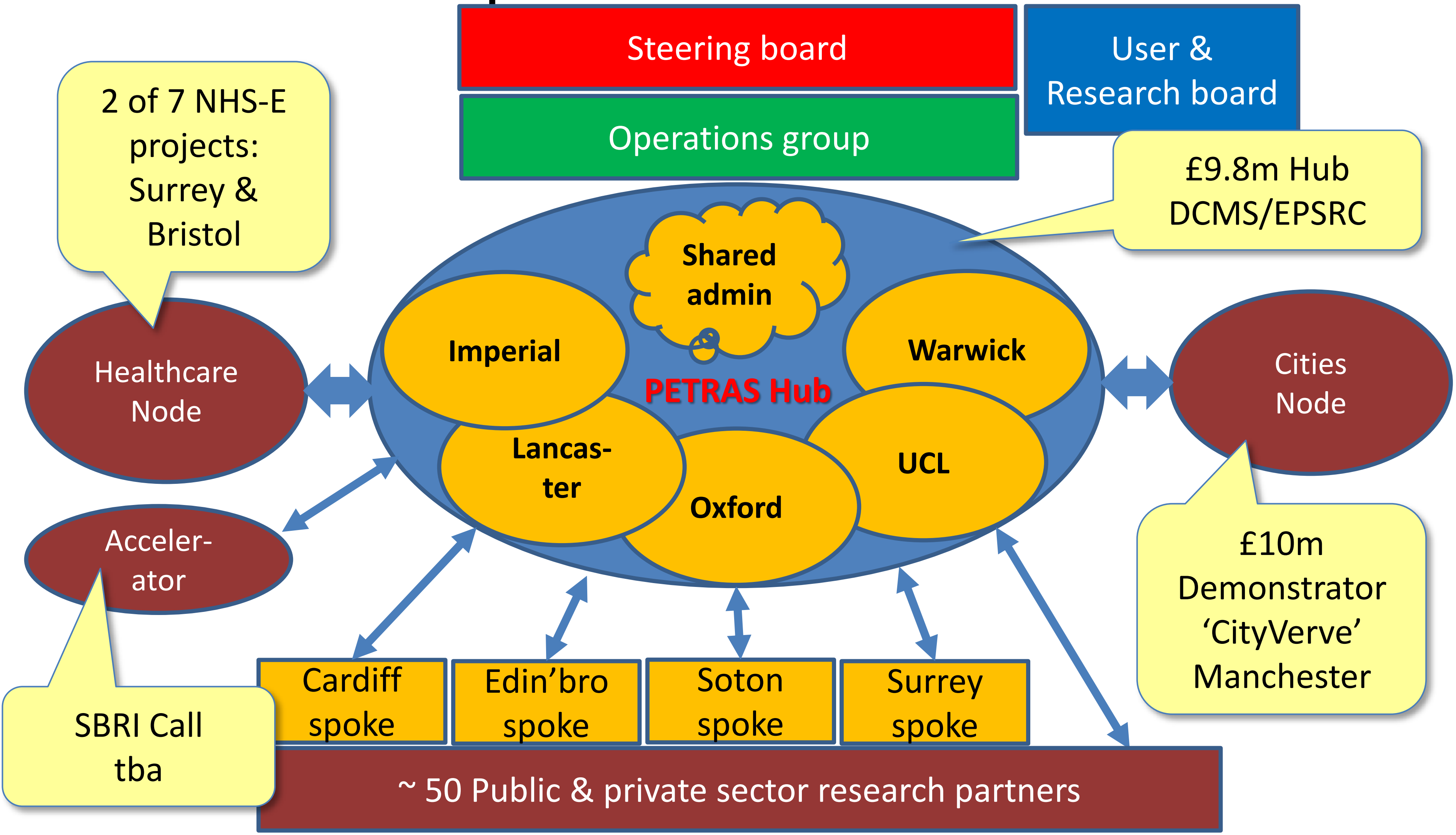
Energy
- Reducing demand
- Matching demand with supply
- Security & standards

Agriculture
- Maximising yield
- Improving food traceability
- Tackling environmental challenges
- Incompatibility
- Lack of infrastructure
- Technical expertise

Buildings
- Optimising design & minimising cost
- Increasing comfort
- Security & safety

⇒ ***Need for focused research & demonstration -> IoTUK***

IoTUK landscape



Steering board

User & Research board

Operations group

£9.8m Hub DCMS/EPSRC

2 of 7 NHS-E projects: Surrey & Bristol

Shared admin

Imperial

Warwick

PETRAS Hub

Lancas-ter

Oxford

UCL

Healthcare Node

Cities Node

Acceler-ator

£10m Demonstrator 'CityVerve' Manchester

SBRI Call tba

Cardiff spoke

Edin'bro spoke

Soton spoke

Surrey spoke

~ 50 Public & private sector research partners

PETR S

PRIVACY, ETHICS, TRUST, RELIABILITY, ACCEPTABILITY, AND SECURITY FOR THE INTERNET OF THINGS

EPSRC

A Research Hub for Cybersecurity of the Internet of Things

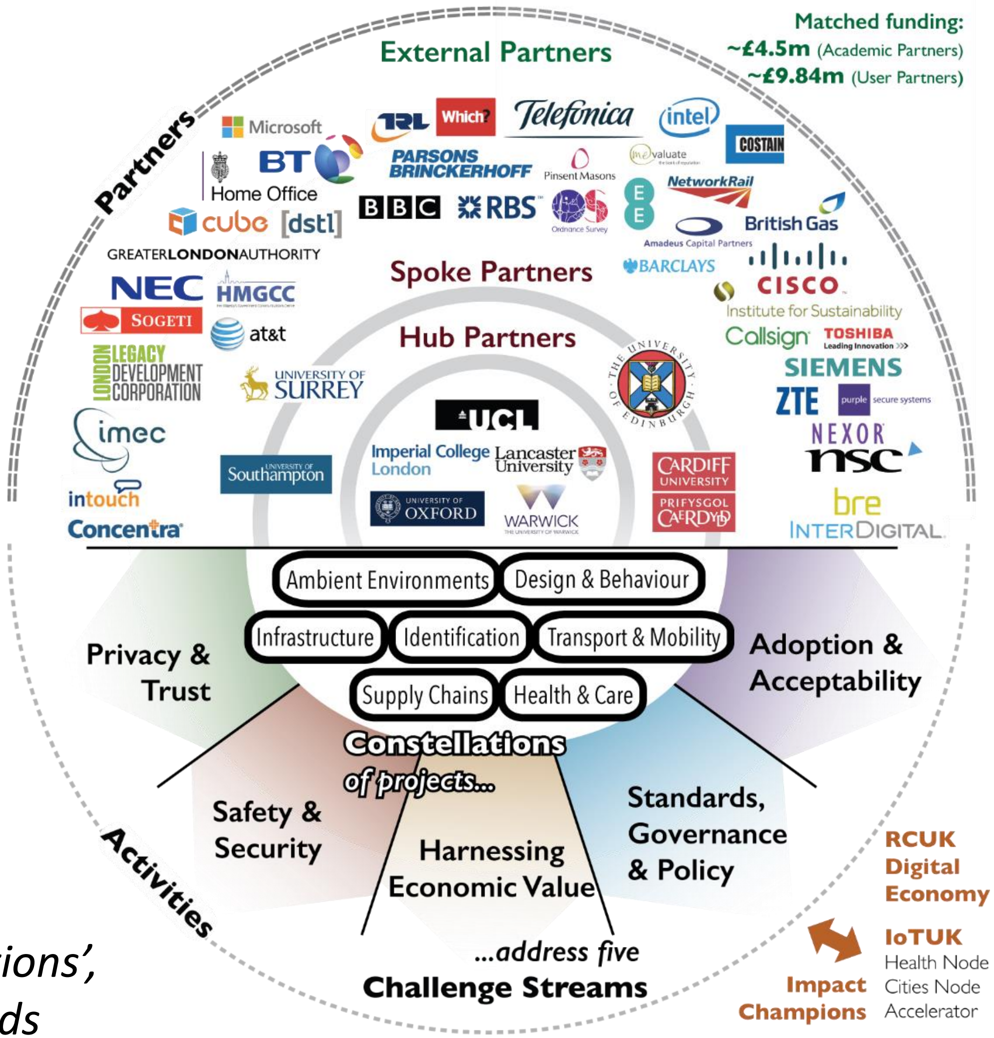
Professor Jeremy Watson CBE FREng
Director and Principal Investigator

UCL · WARWICK · Imperial College London · Lancaster University · University of Oxford · University of Surrey · University of Southampton · The University of Edinburgh · Cardiff University Prifysgol Caerdydd

PETRAS – key facts

- 9 world leading universities via the core and spoke model (4 from the Alan Turing Institute)
- Combined hub value: £24m
- 19 projects at outset, +15 after Phase 2 call
- Blackett Review expertise
- 47 partners at submission, 60+ since, combining presence in the UK, Central Europe and America (giving International links and perspective)
- Inter– and multi-disciplinary focus

Projects grouped by type into 'Constellations', sample one or more of the Stream threads



Matched funding:
~£4.5m (Academic Partners)
~£9.84m (User Partners)

Partners

External Partners

Spoke Partners

Hub Partners

Ambient Environments

Design & Behaviour

Infrastructure

Identification

Transport & Mobility

Supply Chains

Health & Care

Constellations *of projects...*

Privacy & Trust

Adoption & Acceptability

Safety & Security

Harnessing Economic Value

Standards, Governance & Policy

...address five **Challenge Streams**

Activities

RCUK Digital Economy

IoTUK
Health Node
Cities Node
Accelerator

Impact Champions

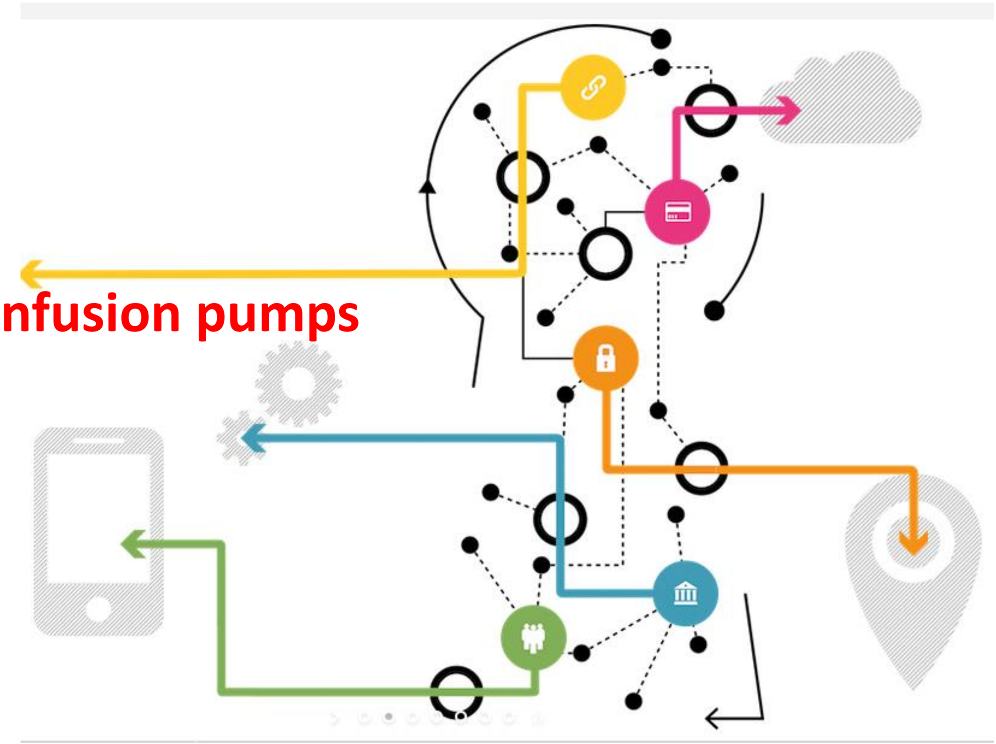
Aims

To:

- Deliver real co-produced cross-sectoral, impactful, and timely **technical and socioeconomic benefit**;
- Place the UK as **world-leader** in expertise and deployment of trusted IoT technology;
- Create a **cross-disciplinary environment** across research domains, industries, and government departments;
- Create a **social platform for innovation** and co-creation with users and stakeholders;
- Provide an **enduring legacy** from the PETRAS Hub, beyond the end of the funded period.

Some examples of threats

- Contactless card skimming
- **Hacking Building Management Systems**
- **Smart toys**
- Baby monitors
- Smart TVs
- USB devices
- **Healthcare devices - Fitbit to infusion pumps**
- Smart domestic goods
- Cars, now and in the future

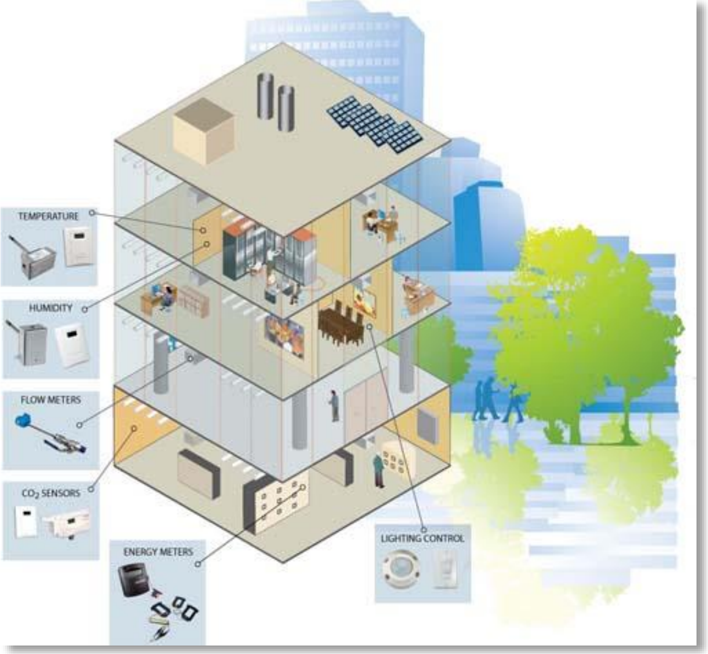


Hacking into Building Management Systems

Disabling a server room chiller can shut a business down

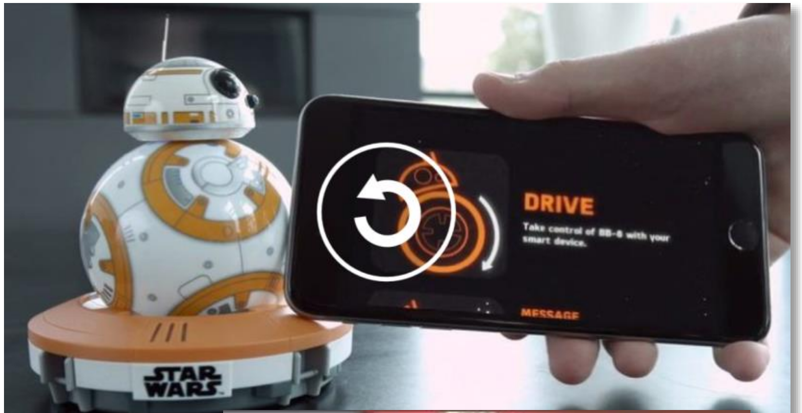
- IBM Ethical Hacking team Pen test
- BMS connected to enterprise IT – a ‘back door’
- Poor ‘Cyberhygiene’ on part of BMS installer – weak password
- Weak router security between BMS and server
- Clear lessons learned

  https://regmedia.co.uk/2016/02/10/567584334543.pdf



Smart Toys

Increasingly, toys are equipped with internet communications, cameras, geolocation, etc.



- Risk of digital stalking and peeping (geolocation with picture data)
- Robots, dolls, drones
- Threat not yet fully emergent, but risk is perceived

See:

http://www.cnet.com/news/hello-headaches-barbie-of-the-internet-age-has-even-more-security-flaws/

Healthcare devices

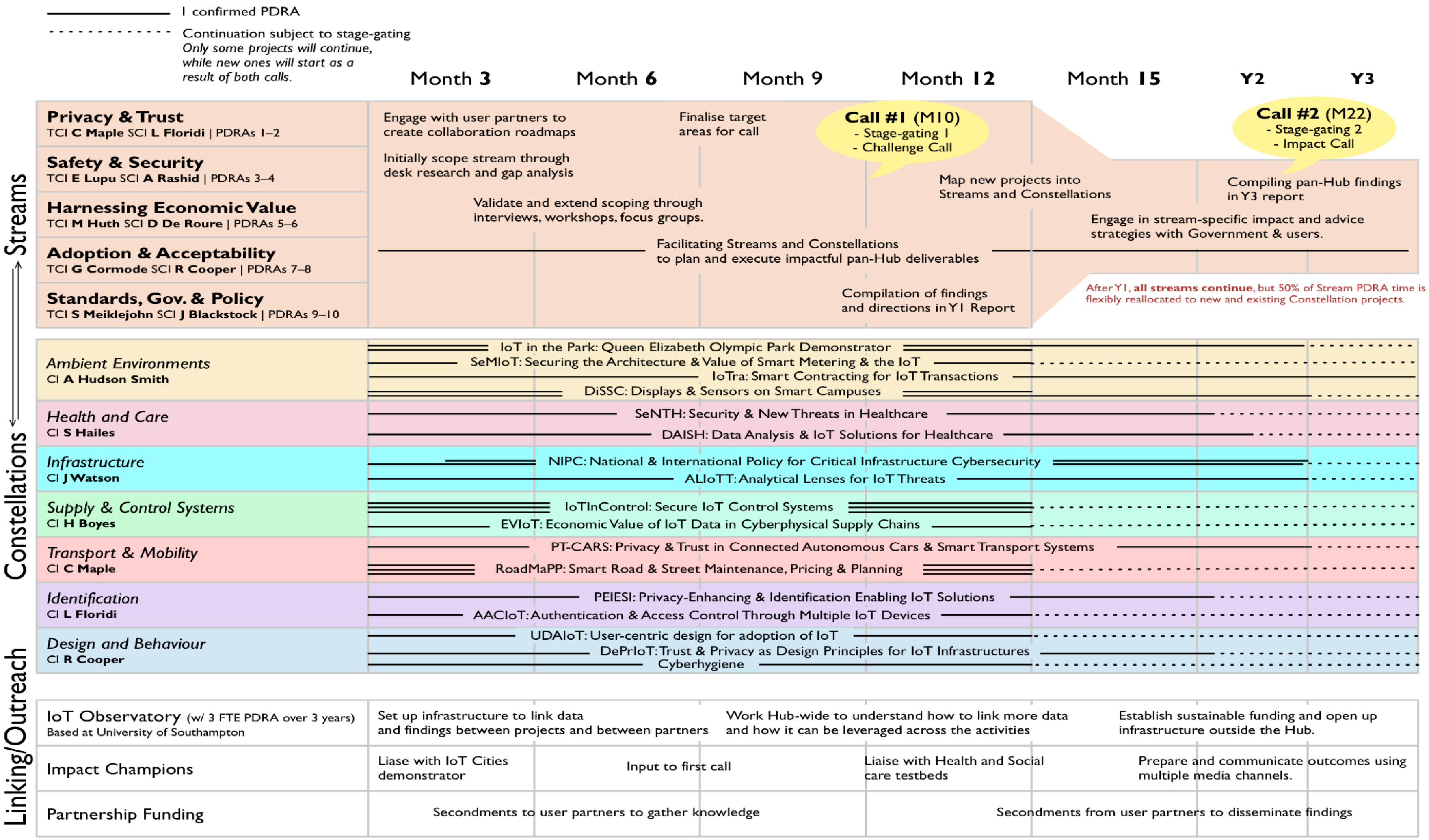
Wide range of applications – from low importance leisure to life-critical

- Risks range from telehealth data theft to life-threatening adjustments of critical personal support equipment

- Telehealth devices typically use short-range communication or wired connection

- Implanted systems, like heart pacemakers are adjusted by low frequency near-field communications

The PETRAS work plan



I confirmed PDRA

Continuation subject to stage-gating
Only some projects will continue, while new ones will start as a result of both calls.

Month 3 | Month 6 | Month 9 | Month 12 | Month 15 | Y2 | Y3

Streams

Privacy & Trust
TCI **C Maple** SCI **L Floridi** | PDRAs 1–2

Safety & Security
TCI **E Lupu** SCI **A Rashid** | PDRAs 3–4

Harnessing Economic Value
TCI **M Huth** SCI **D De Roure** | PDRAs 5–6

Adoption & Acceptability
TCI **G Cormode** SCI **R Cooper** | PDRAs 7–8

Standards, Gov. & Policy
TCI **S Meiklejohn** SCI **J Blackstock** | PDRAs 9–10

Engage with user partners to create collaboration roadmaps

Finalise target areas for call

Call #1 (M10)
- Stage-gating 1
- Challenge Call

Initially scope stream through desk research and gap analysis

Validate and extend scoping through interviews, workshops, focus groups.

Facilitating Streams and Constellations to plan and execute impactful pan-Hub deliverables

Compilation of findings and directions in Y1 Report

Map new projects into Streams and Constellations

Engage in stream-specific impact and advice strategies with Government & users.

Call #2 (M22)
- Stage-gating 2
- Impact Call

Compiling pan-Hub findings in Y3 report

After Y1, **all streams continue**, but 50% of Stream PDRA time is flexibly reallocated to new and existing Constellation projects.

Constellations

Ambient Environments
CI **A Hudson Smith**
- IoT in the Park: Queen Elizabeth Olympic Park Demonstrator
- SeMIoT: Securing the Architecture & Value of Smart Metering & the IoT
- IoTra: Smart Contracting for IoT Transactions
- DiSSC: Displays & Sensors on Smart Campuses

Health and Care
CI **S Hailes**
- SeNTH: Security & New Threats in Healthcare
- DAISH: Data Analysis & IoT Solutions for Healthcare

Infrastructure
CI **J Watson**
- NIPC: National & International Policy for Critical Infrastructure Cybersecurity
- ALIoTT: Analytical Lenses for IoT Threats

Supply & Control Systems
CI **H Boyes**
- IoTInControl: Secure IoT Control Systems
- EVIoT: Economic Value of IoT Data in Cyberphysical Supply Chains

Transport & Mobility
CI **C Maple**
- PT-CARS: Privacy & Trust in Connected Autonomous Cars & Smart Transport Systems
- RoadMaPP: Smart Road & Street Maintenance, Pricing & Planning

Identification
CI **L Floridi**
- PEIESI: Privacy-Enhancing & Identification Enabling IoT Solutions
- AACIoT: Authentication & Access Control Through Multiple IoT Devices

Design and Behaviour
CI **R Cooper**
- UDAIoT: User-centric design for adoption of IoT
- DePrIoT: Trust & Privacy as Design Principles for IoT Infrastructures
- Cyberhygiene

Linking/Outreach

IoT Observatory (w/ 3 FTE PDRA over 3 years)
Based at University of Southampton
- Set up infrastructure to link data and findings between projects and between partners
- Work Hub-wide to understand how to link more data and how it can be leveraged across the activities
- Establish sustainable funding and open up infrastructure outside the Hub.

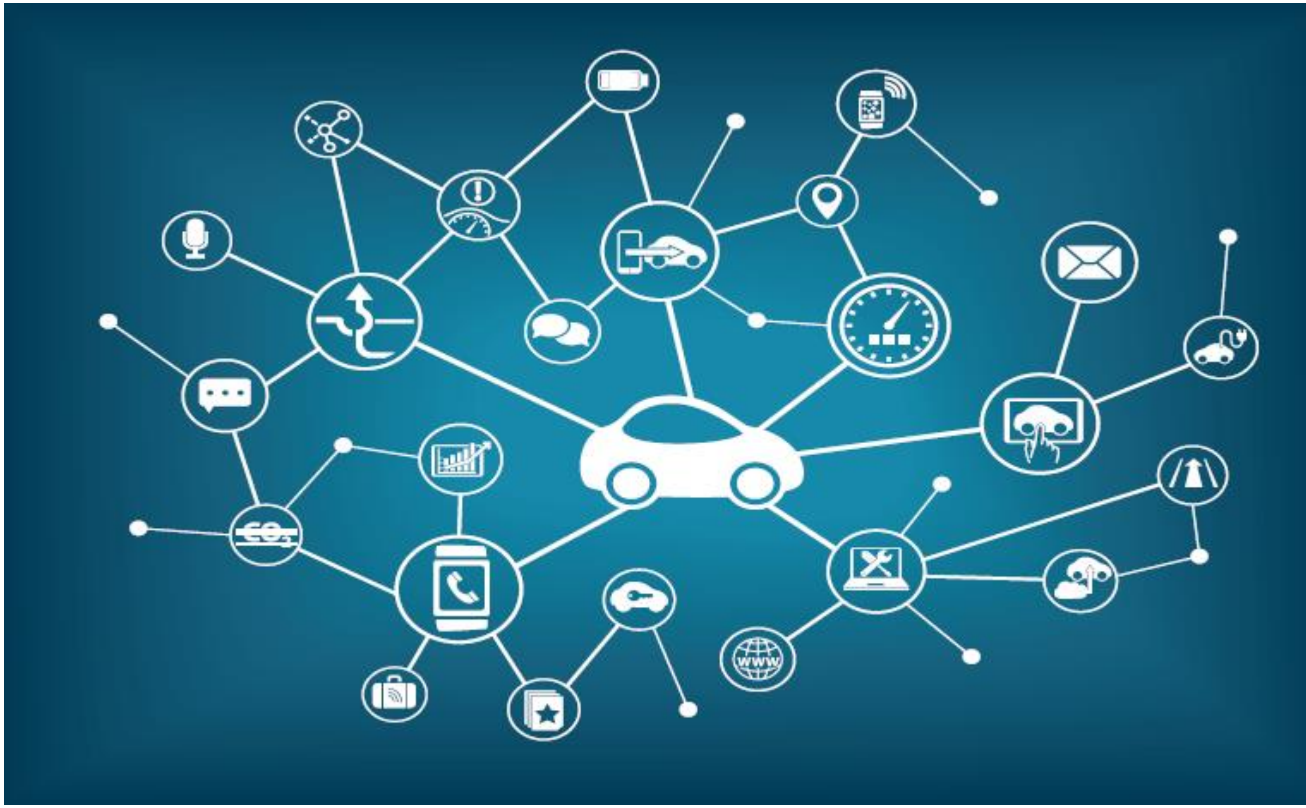
Impact Champions
- Liase with IoT Cities demonstrator
- Input to first call
- Liaise with Health and Social care testbeds
- Prepare and communicate outcomes using multiple media channels.

Partnership Funding
- Secondments to user partners to gather knowledge
- Secondments from user partners to disseminate findings

Constellation example: Transport & Mobility

Transport & Mobility projects will include
smart street planning, pricing & maintenance and also developing solutions for communications among autonomous and semi-autonomous cars and infrastructures.

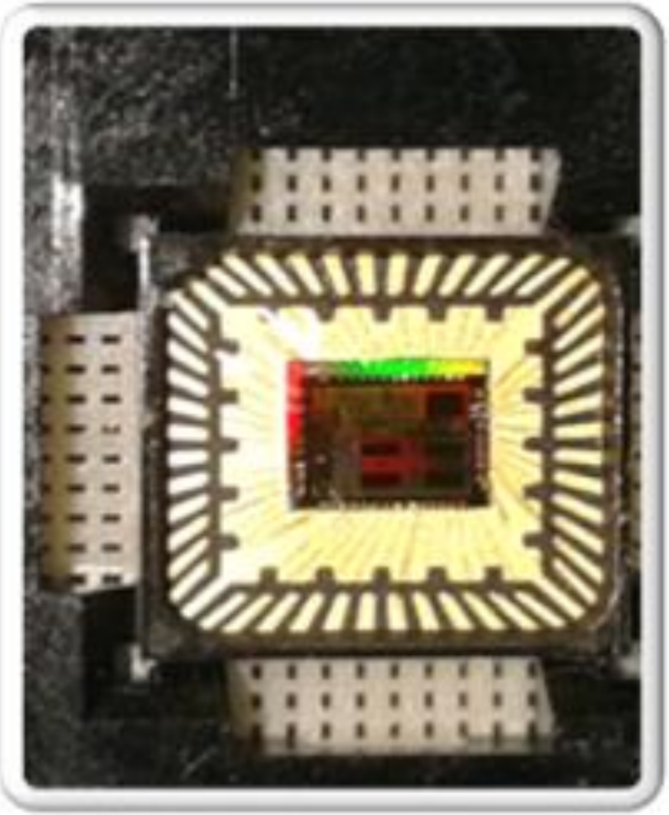
Lead: Professor Carsten Maple (Warwick)



Constellation example: Health & Care

SeNTH - focus on: 1. Threat modelling and analysis for body sensor networks; 2. Security mechanisms that can be provided on miniaturised low power ASICs; 3. Establishing a test-bed with selected scenarios. DASH - user trust in medical applications of IoT. Project will use sandpits to identify problems impairing users' trust and will define a code of practises for IoT.

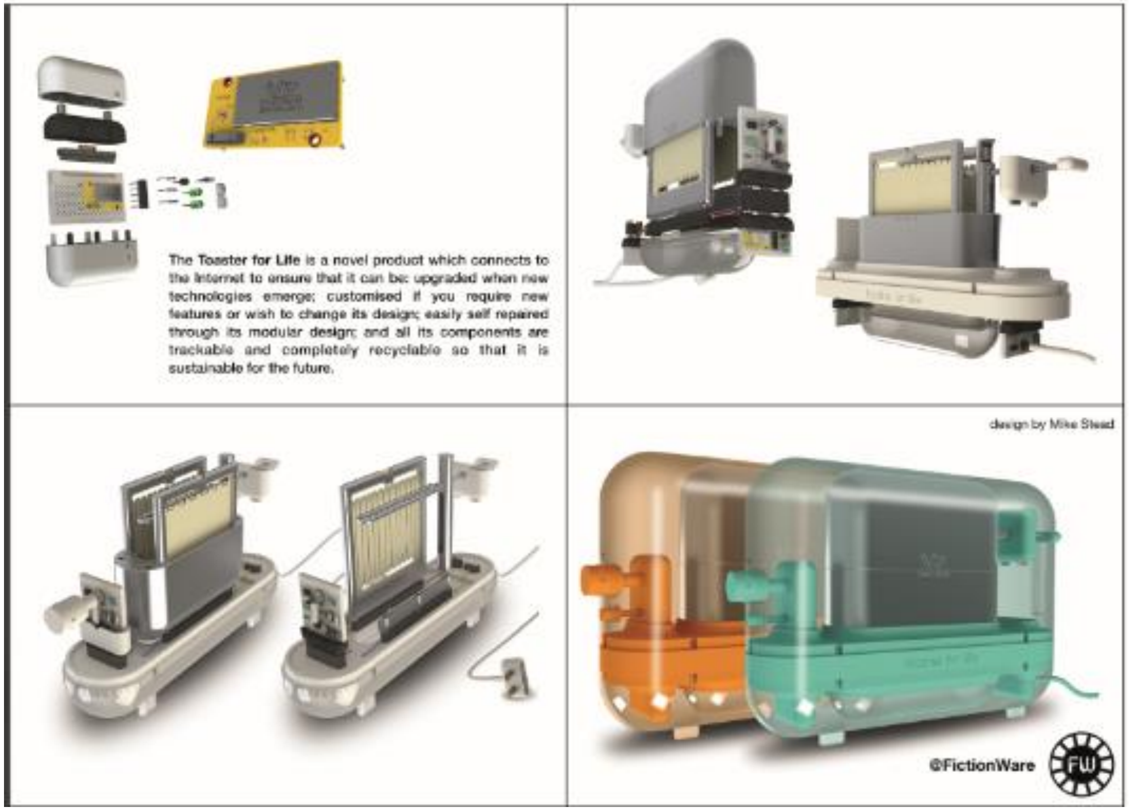
Lead: Emil Lupu (Imperial College)



Constellation example: Design & Behaviour

This Constellation will consider the role that Design plays in influencing the adoption of IoT. In particular, how Design and Engineering can actively encourage or discourage behaviours, so that Privacy and Trust are enhanced, and adoption is promoted. Design charrettes will be used to obtain user responses to a range of interventions.

Lead: Professor Rachel Cooper (Lancaster)



The Toaster for Life is a novel product which connects to the Internet to ensure that it can be upgraded when new technologies emerge; customised if you require new features or wish to change its design; easily self repaired through its modular design; and all its components are trackable and completely recyclable so that it is sustainable for the future.

Constellation example: Infrastructure

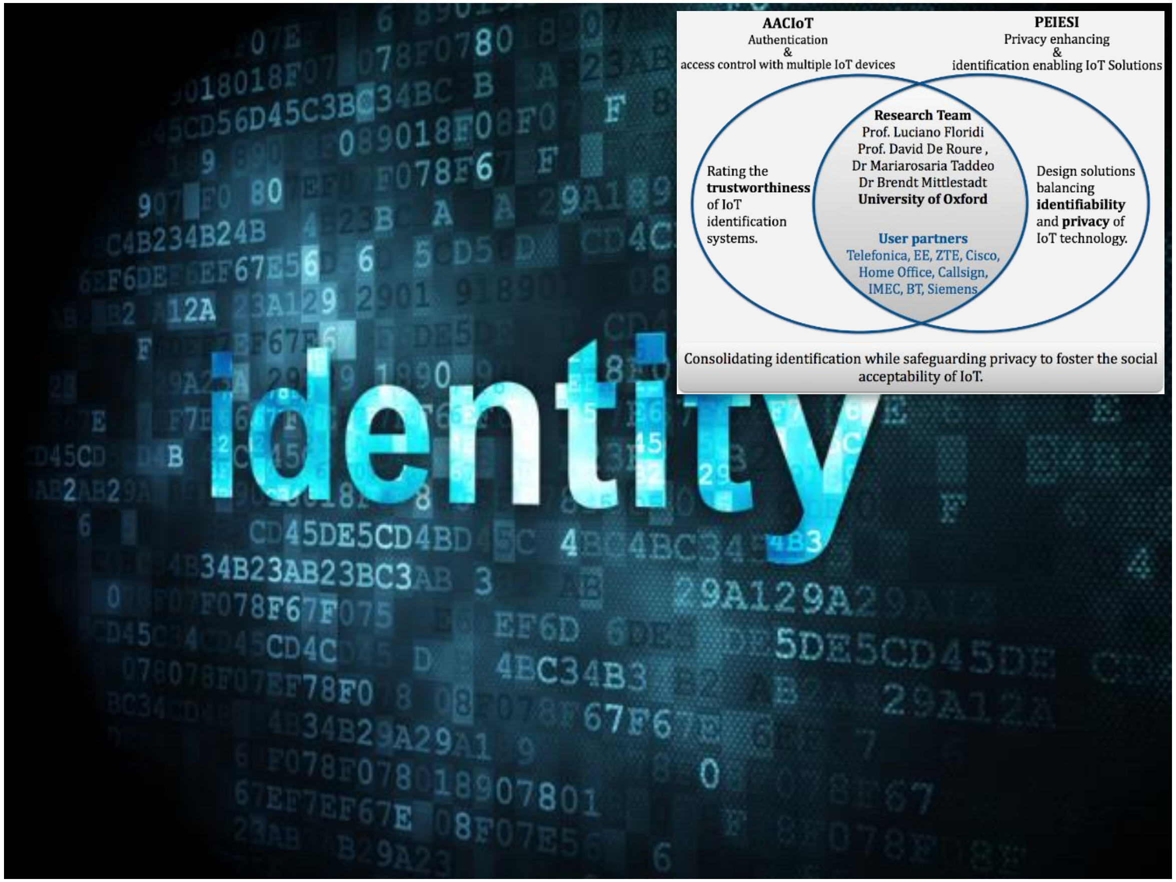
Includes 1. NIRC, which looks, from a policy angle, at approaches in various countries and across borders to manage IoT threats and increased attack surfaces. 2. ALIoTT - tools to analyse threats in many contexts, creating, validating and piloting methods and software across the hub and with User Partners, including government agencies.

Lead: Professor Jeremy Watson (UCL)

Constellation example: Identification

AACIoT - rating the trustworthiness of identification systems based on the wider environment surrounding the IoT agent PEISI evaluating ‘identifying’ technologies, protocols, and procedures alongside privacy strategies, to design robust solutions that deliver a balance between identifiability and privacy of IoT technology.

Lead: Professor Luciano Floridi (Oxford)



AACIoT
Authentication
&
access control with multiple IoT devices

PEIESI
Privacy enhancing
&
identification enabling IoT Solutions

Rating the **trustworthiness** of IoT identification systems.

Research Team
Prof. Luciano Floridi
Prof. David De Roure ,
Dr Mariarosaria Taddeo
Dr Brendt Mittlestadt
University of Oxford

User partners
Telefonica, EE, ZTE, Cisco, Home Office, Callsign, IMEC, BT, Siemens

Design solutions balancing **identifiability** and **privacy** of IoT technology.

Consolidating identification while safeguarding privacy to foster the social acceptability of IoT.

Constellation example: Supply & Control Systems

Connectivity and intelligence are of economic importance to the UK. IoT offers integrated control systems and supply chains. Projects include: Developing Secure IoT-augmented Control Systems and Exploring Economic Value of IoT Data in Cyber-physical Supply Chains. The projects will draw expertise from a number of Hub research organisations working with industrial partners.

Lead: Professor Carsten Maple (Warwick)

Constellation example: Ambient Environments

The QEOP offers an ideal setting for scalable, ‘In the Wild’, IoT developments. Concepts around security versus adaptability with cross-layered network wide protocols for low powered IoT Devices will be investigated . A combination of In the Wild experiments and focus groups will inform the boundaries of privacy, trust and personalisation.

Lead: Professor Andy Hudson-Smith (UCL)

New projects – Strategic Research Fund

Filling first-round research gaps identified by state-of-the art and gap analysis studies

- **IoT Security for Healthcare (SeNTH +)** – Imperial, Intel
- **Modelling the potential impact of IoT boosted botnet attacks (BotThings)** – UCL, NCCU
- **Developing a Consumer Security Index for Domestic IoT devices** – UCL, Met Police, Which?, Dawes Centre, BIT
- **The Internet of Energy Things: supporting peer-to-peer energy trading and demand side management through blockchains. (P2P-IoET)** – UCL, Siemens, UKPN
- **Security Risk Assessment of IoT Environments with Attack Graph Models** – Imperial, BRE
- **Resolving Conflicts in Public Spaces** – Surrey, Rail Delivery Group, RSSB

New projects – Strategic Research Fund

Filling first-round research gaps identified by state-of-the art and gap analysis studies

- **Respectful Things in Private Spaces: Investigating Ethical Data Handling for Very Personal Devices** – Oxford, BT
- **Value of Personal Data in IoT** – Warwick, Met Police, BT, Which?, Digital Catapult
- **Smart Meter Code of Practice (HANCODE)** – Warwick, EDF
- **Hybrid Engagement Architecture Layer for Trusted Human-Centric IoT** – Southampton, CityVerve, Southampton City Council, Siemens, Zooniverse
- **Resilience and security in Low Power IoT** – UCL, IBM (UK)
- **Designing Dynamic Insurance Policies Using IoT** – Imperial, Lloyds Register Foundation
- **Blockchain-empowered Infrastructure for IoT (BlockIT)** – Southampton, British Gas, DSTL, Lloyds Register Foundation

New projects – Strategic Research Fund

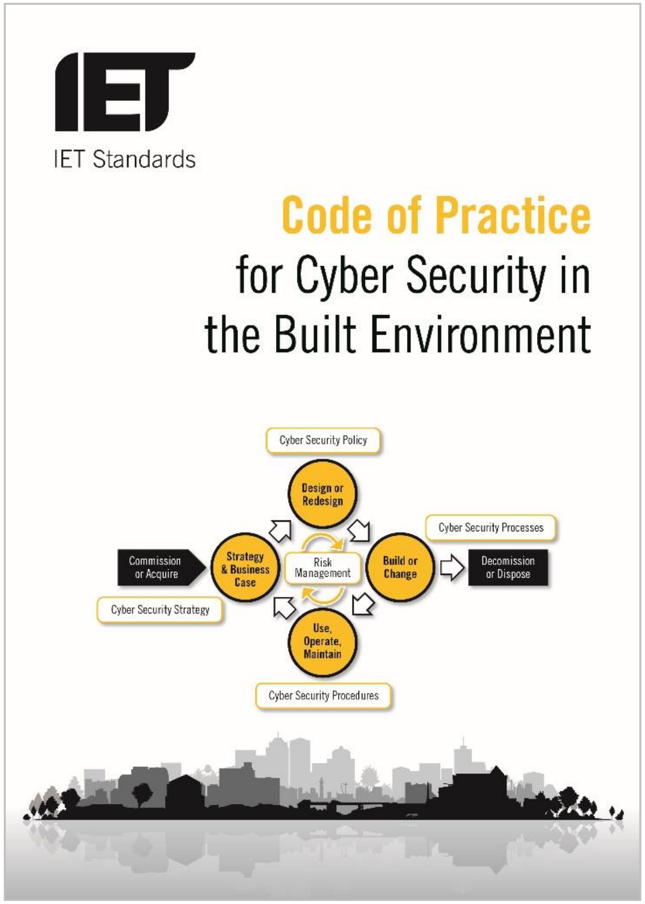
Filling first-round research gaps identified by state-of-the art and gap analysis studies

- **Identifying Attack Vectors for Network Intrusion via IoT devices & Developing a Goal-Oriented Approach to Determining Impact Across Threat Surfaces (IoT Depends)** – Cardiff, Airbus, Lloyds Register Foundation
- **Blockchain Technology for IoT in Intelligent Transportation Systems (B-IoT)** – Imperial, Ordnance Survey, Wallet Services

Links

- BIM Level 2 – PAS 1192: http://shop.bsigroup.com/Navigate-by/PAS/PAS-1192-22013/
- Digital Built Britain: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/410096/bis-15-155-digital-built-britain-level-3-strategy.pdf
- Home Office produced an interactive PDF advice document in light of findings of a recent Ministerial Roundtable: https://www.gov.uk/government/publications/internet-of-things-potential-risk-of-crime-and-how-to-prevent-it
- Blackett Review: The Internet of Things: making the most of the Second Digital Revolution: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/409774/14-1230-internet-of-things-review.pdf
- Petras Hub: https://www.petrashub.org/

IET Cyber Security and IoT activities



IET Standards

Code of Practice for Cyber Security in the Built Environment

Security Series 2

Engineering Secure Internet Of Things Systems

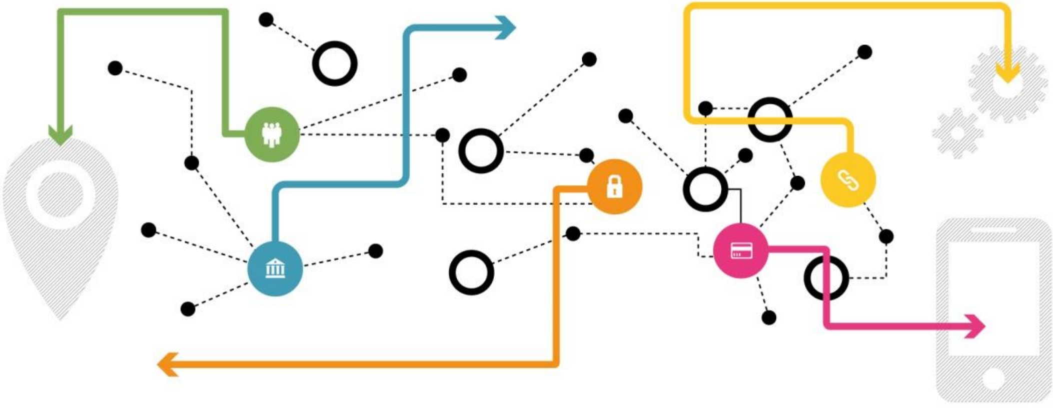
Edited by Benjamin Aziz, Alvaro Arenas and Bruno Crispo

Living in the Internet of Things:

Cybersecurity of the IoT - A PETRAS, IoTUK & IET Event

28 – 29 March 2018 | IET London: Savoy Place

Addressing the cybersecurity of the **Internet of Things** and exploring critical issues in privacy, ethics, trust, reliability, acceptability, and security through both social science and technical disciplines.



Call for papers deadline: 10 November 2017

www.theiet.org/cyberiot

PETRAS iot UK

The Institution of Engineering and Technology

Working to engineer a better world

Thank you

The Institution of Engineering and Technology

UCL

From digitization to digital innovations

Dr Bethan Morgan

September 2017

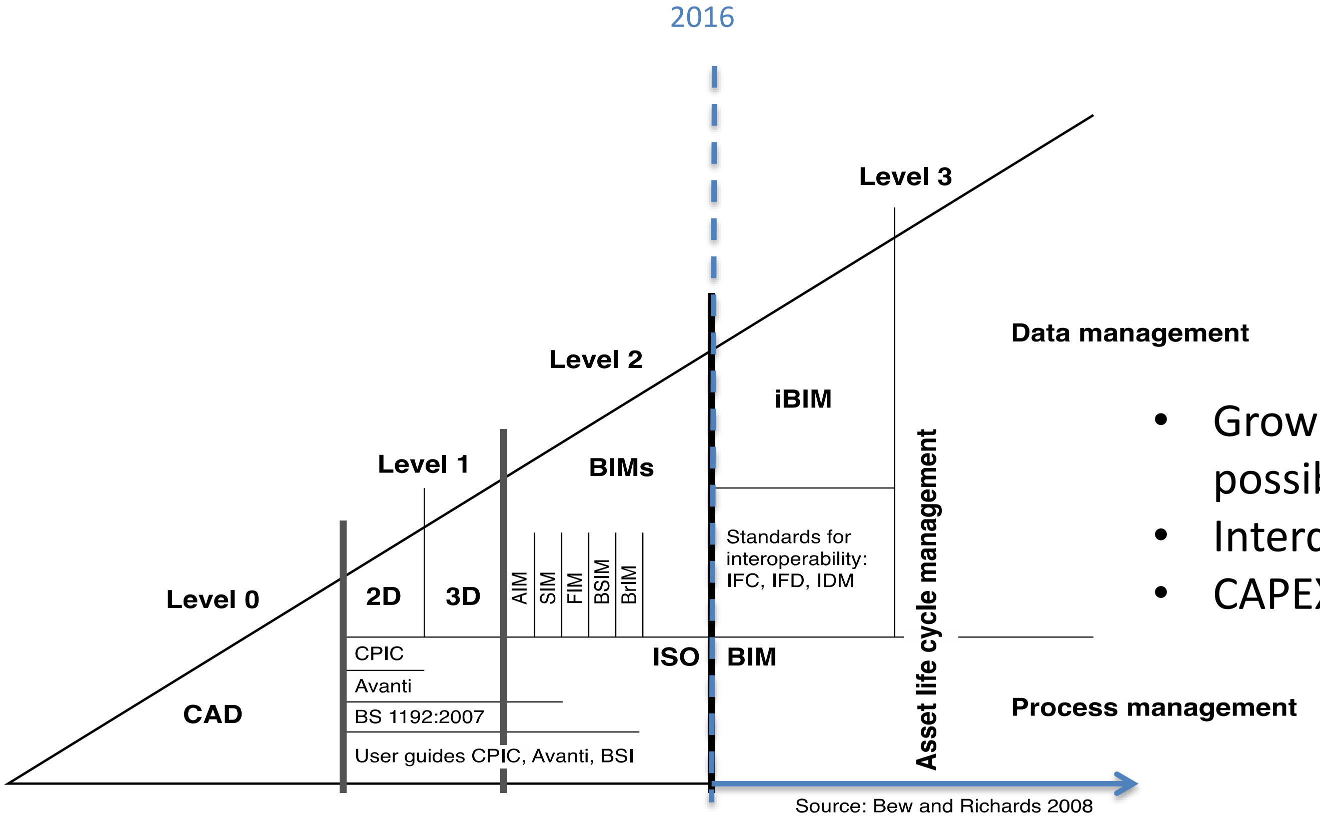
EPSRC

Engineering and Physical Sciences Research Council

Background

- Accelerating pace of digitization
  - What might it mean for construction?
- Digital innovations
  - Value is in how we use technologies
  - Digital innovation, not invention

Technological change

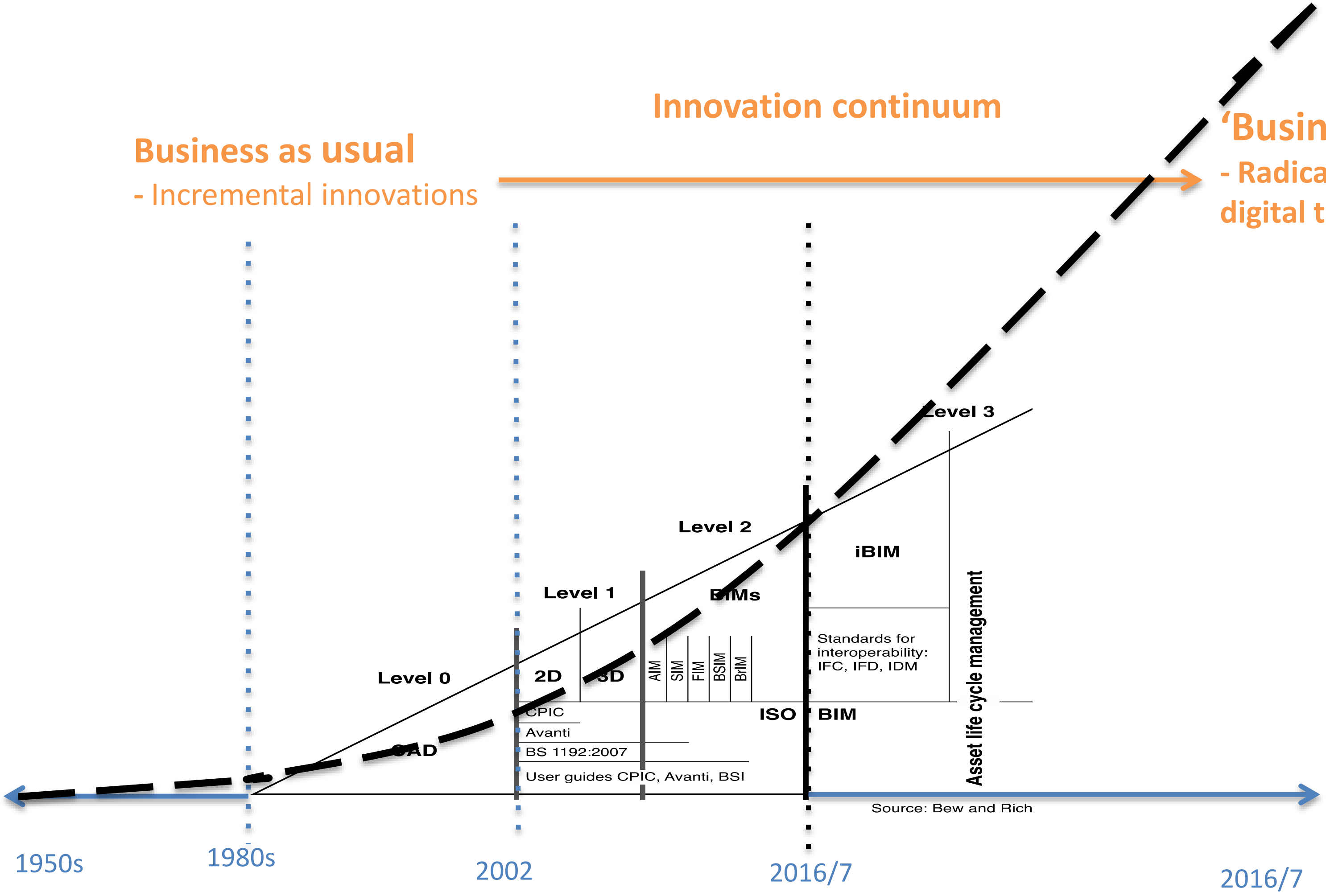


Source: Bew and Richards 2008

- Growing digital possibilities
- Interdependencies
- CAPEX to OPEX

September 2017

Accelerating rate of digitization


Innovation continuum
Business as usual
- Incremental innovations
'Business as unusual'
- Radical, potentially disruptive, digital technologies
Level 3
Level 2
Level 1
Level 0
iBIM
BIMs
2D
3D
CAD
AIM
SIM
FIM
BSIM
BrIM
Standards for interoperability: IFC, IFD, IDM
ISO
BIM
CPIC
Avanti
BS 1192:2007
User guides CPIC, Avanti, BSI
Asset life cycle management
1950s
1980s
2002
2016/7
2016/7

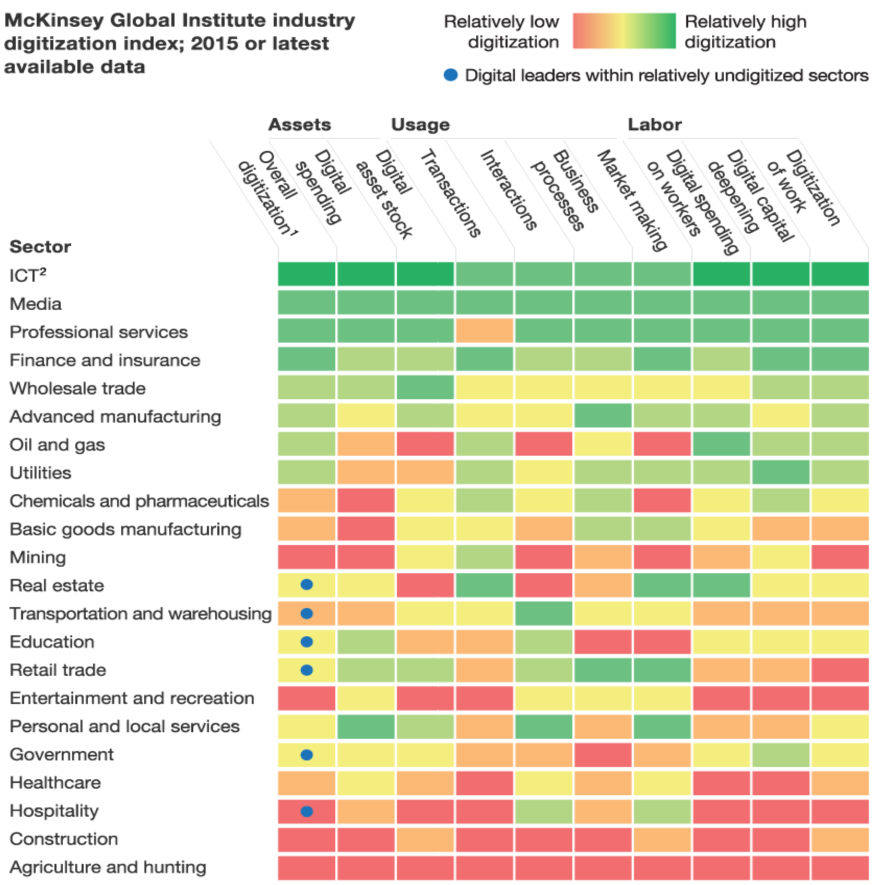
Source: Bew and Rich

September 2017

From digitization to digital innovations

‘Ripe for disruption’

The construction industry is among the least digitized.


McKinsey Global Institute industry digitization index; 2015 or latest available data

[1] Based on a set of metrics to assess digitization of assets (8 metrics), usage (11 metrics), and labor (8 metrics).

[2] Information and communications technology.

Source: AppBrain; Bluewolf; Computer Economics; eMarketer; Gartner; IDC Research; LiveChat; US Bureau of Economic Analysis; US Bureau of Labor Statistics; US Census Bureau; McKinsey Global Institute analysis

McKinsey&Company

Sources of digitization

- Last 24 months, 12 major reports (so far …)
- Additive manufacturing, AI / robotics, automation, advanced materials, smart technologies, big data, VR / AR, advanced applications of BIM (OPEX)
- Applications of these already apparent
  - Technologies used in combination
  - Wider business changes

Digitization and digitalization

- Digitalization is the challenge for construction
  - similar term, very different meaning
  - wider than digitization
  - embraces social, regulatory and business model change
- Key challenge for construction
  - the industry doesn’t invent technologies, it imports them

Digital innovations

- Innovation is the application of new ideas
- Therefore using / applying technologies is a key digital capability.

- "The inherent value of a technology remains latent until it is commercialized in some way”

(Chesbrough and Rosenbloom, 2000)

USING DIGITAL IN CONSTRUCTION

DAVID DONALDSON (BIM MANAGER)

& PATRICK OWEN (ASSET INFORMATION MANAGER)

19 SEPTEMBER 2017

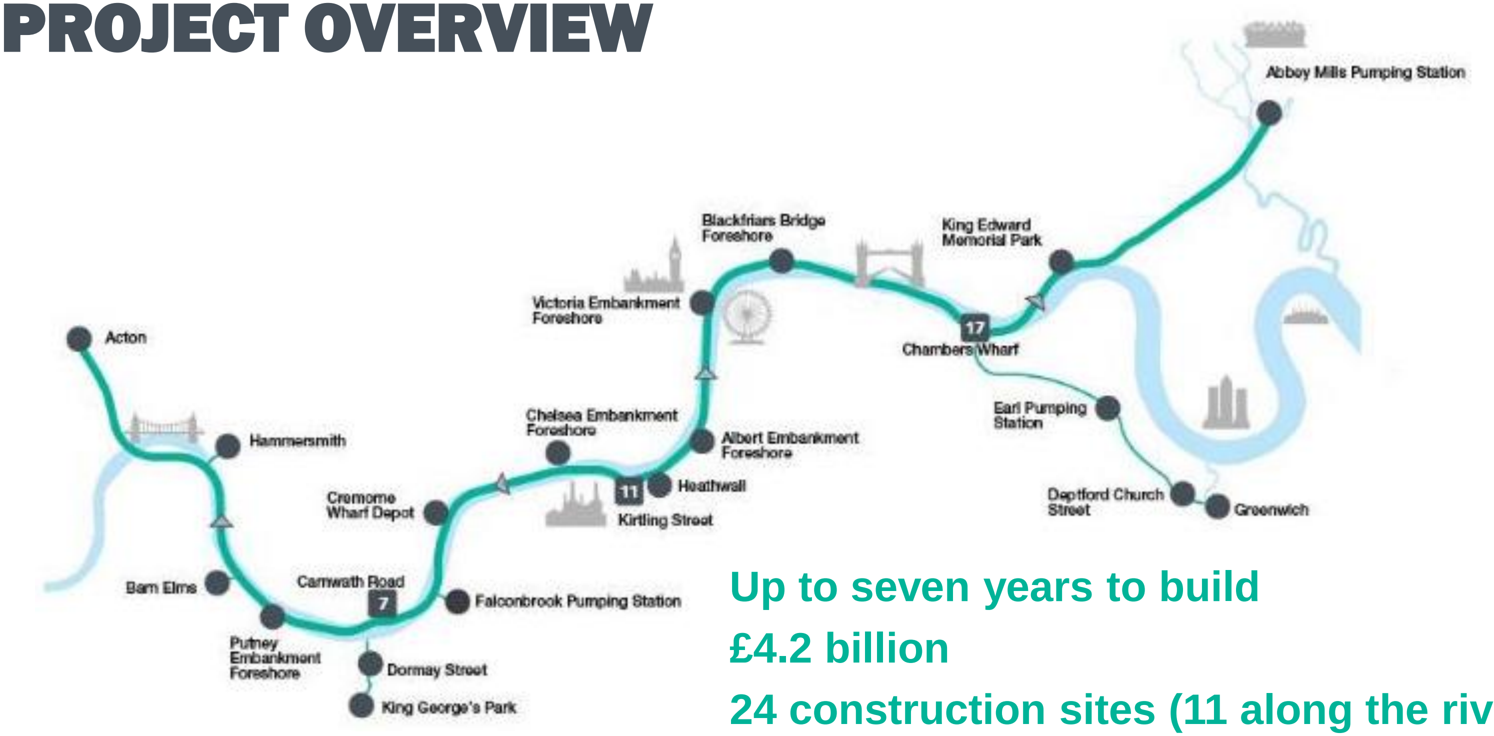
Tideway

USING DIGITAL IN CONSTRUCTION

A BRIEF INTRODUCTION TO TIDEWAY

A BRIEF INTRODUCTION TO TIDEWAY

PROJECT OVERVIEW


Abbey Mills Pumping Station
Blackfriars Bridge Foreshore
King Edward Memorial Park
Victoria Embankment Foreshore
Acton
17
Chambers Wharf
Earl Pumping Station
Chelsea Embankment Foreshore
Albert Embankment Foreshore
Hammersmith
Heathwall
11
Kirtling Street
Cremorne Wharf Depot
Deptford Church Street
Greenwich
Barn Elms
Carnwath Road
7
Falconbrook Pumping Station
Putney Embankment Foreshore
Dormay Street
King George's Park

Up to seven years to build

£4.2 billion

24 construction sites (11 along the river)

2007/14
Planning

2015
Preparation

2016
Construction begins

2017
Tunnelling commences

2021
Tunnelling Ends

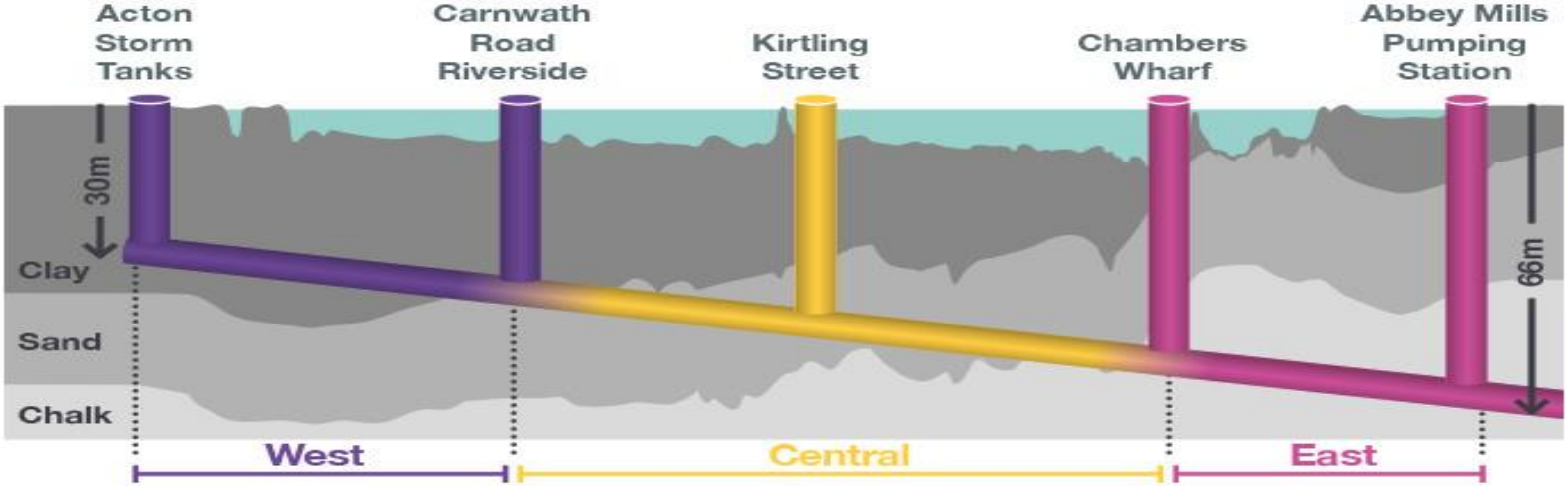
2022
Construction completion

2023/24
System commissioning

A BRIEF INTRODUCTION TO TIDEWAY

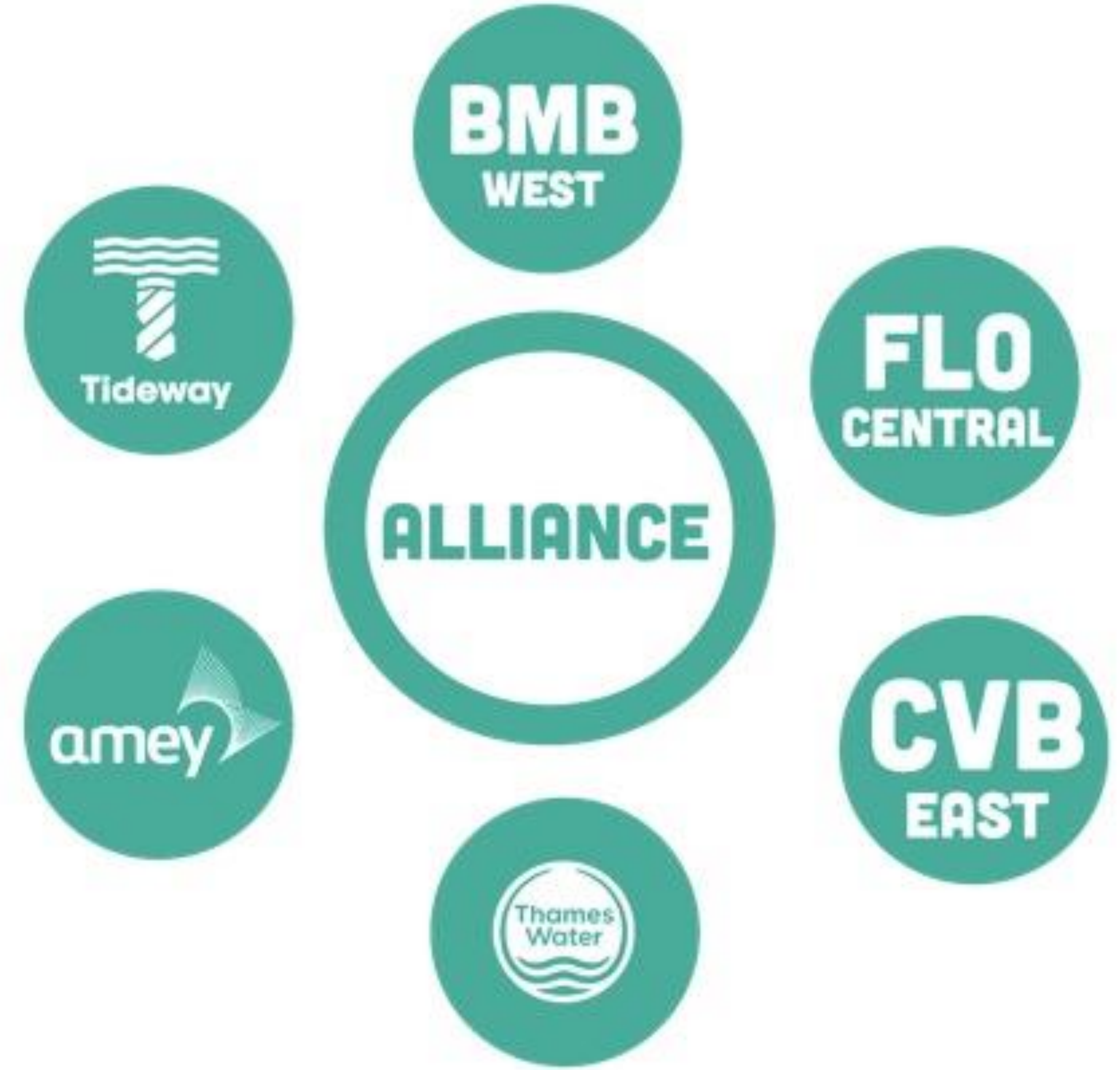
MAIN CONTRACTORS

West BMB JV	Central FLO JV	East CVB JV	System Integrator
bam nuttall MORGAN SINDALL Balfour Beatty	ferrovial agroman LAING O'ROURKE	VINCI CONSTRUCTION BACHY SOLETANCHE COSTAIN	amey



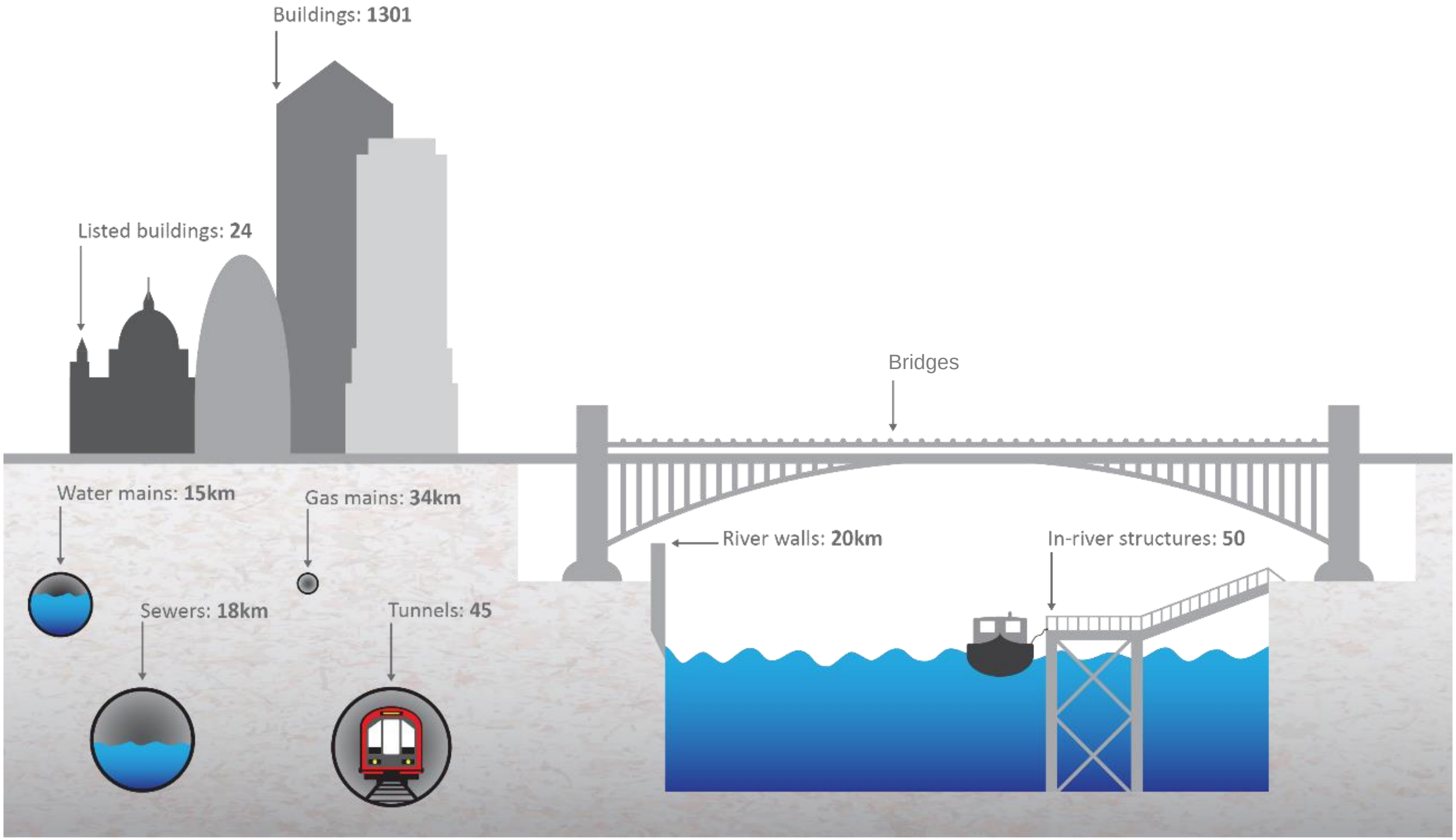
A BRIEF INTRODUCTION TO TIDEWAY

TIDEWAY ALLIANCE



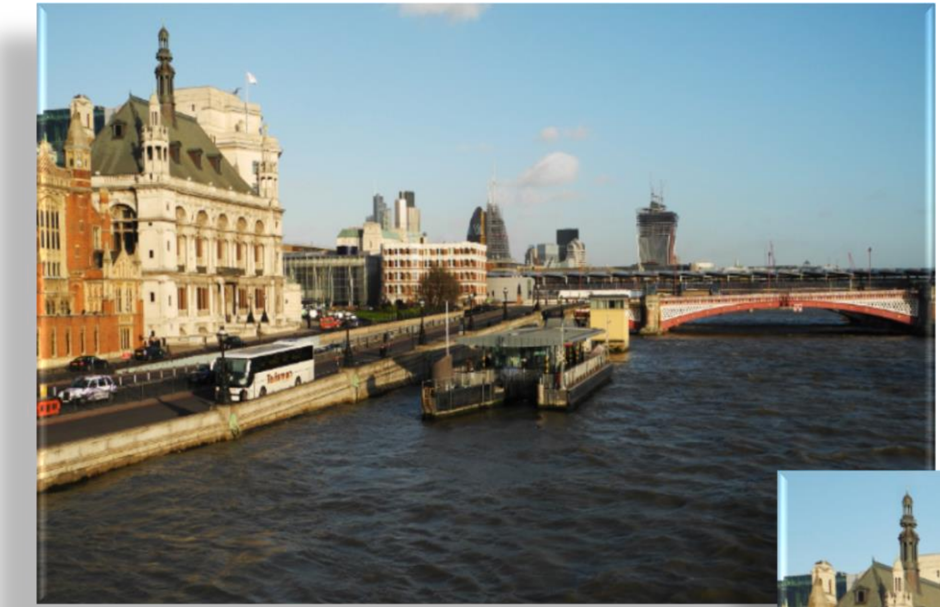
A BRIEF INTRODUCTION TO TIDEWAY

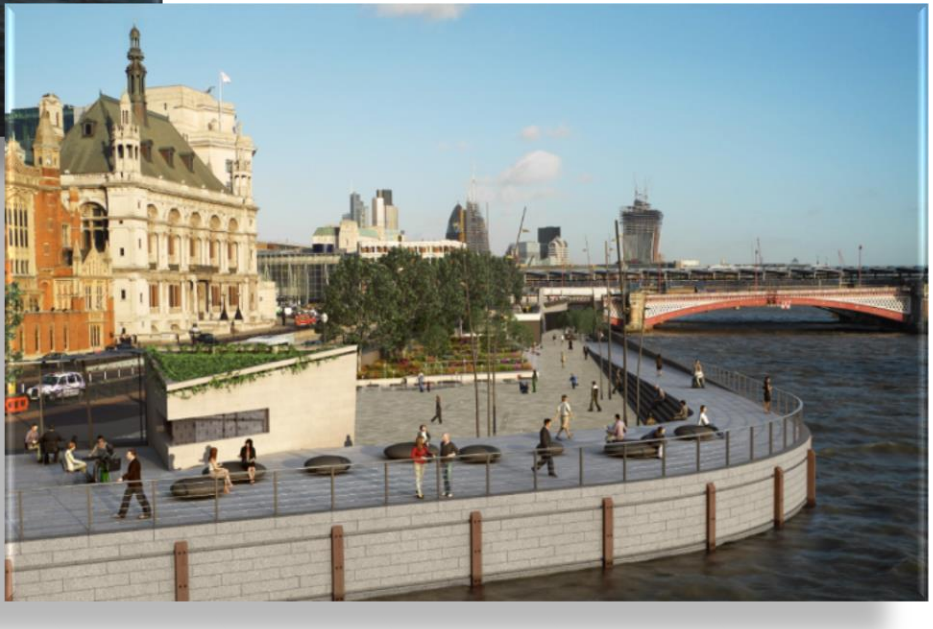
INTERFACES WITH EXISTING INFRASTRUCTURE



A BRIEF INTRODUCTION TO TIDEWAY

PUBLIC REALM: BEFORE & AFTER



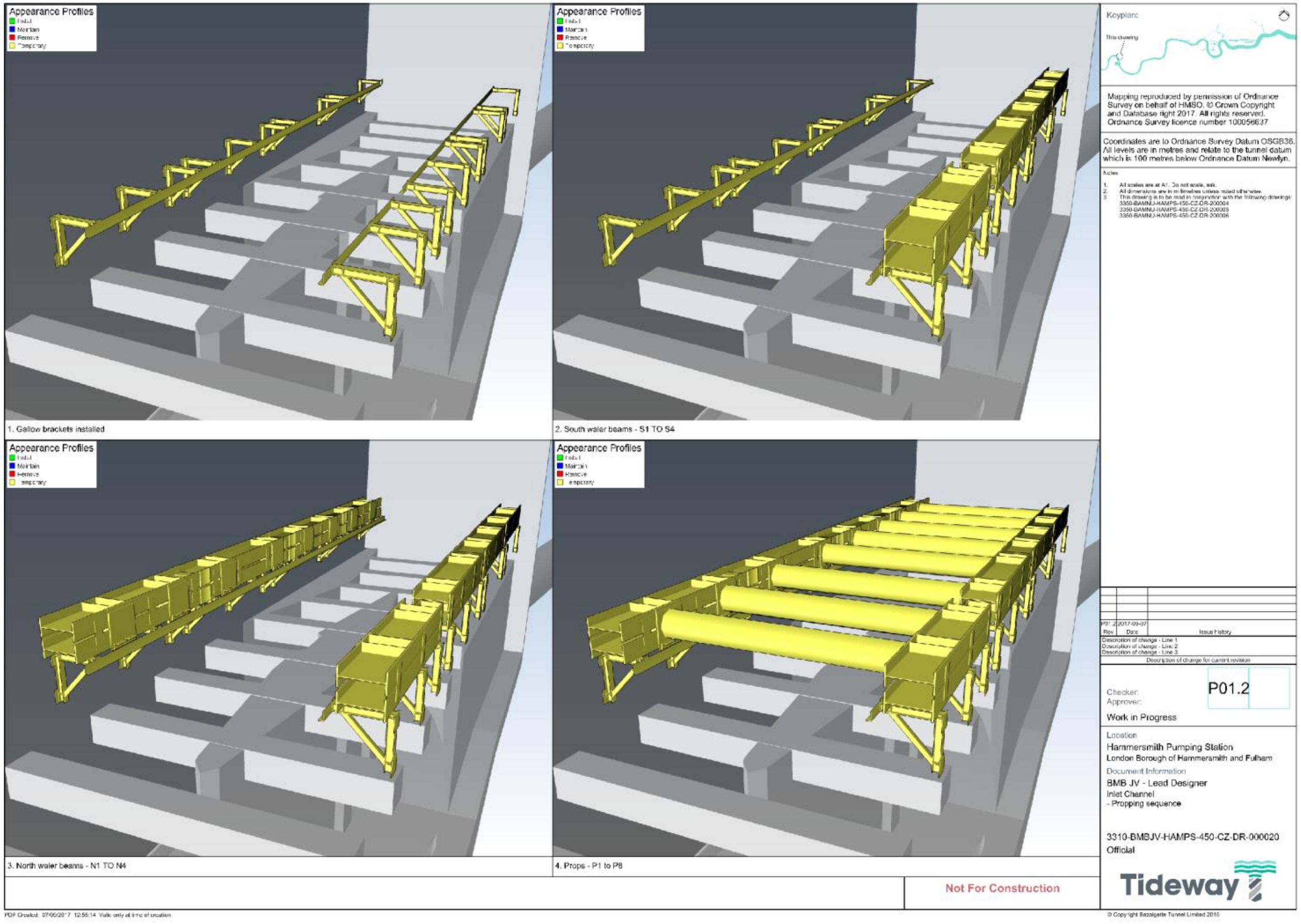


USING DIGITAL IN CONSTRUCTION

EXAMPLES OF WHERE DIGITAL IS BEING USED

EXAMPLES OF WHERE DIGITAL IS BEING USED

INLET CHANNEL – PROPPING SEQUENCE



1. Gallow brackets installed

2. South waler beams - S1 TO S4

3. North waler beams - N1 TO N4

4. Props - P1 to P8

Mapping reproduced by permission of Ordnance Survey on behalf of HMSO. © Crown Copyright and Database right 2017. All rights reserved. Ordnance Survey licence number 100056637

Coordinates are to Ordnance Survey Datum OSGB36. All levels are in metres and relate to the tunnel datum which is 100 metres below Ordnance Datum Newlyn.

Notes

1. All scales are at A1. Do not scale, ask.
2. All dimensions are in millimetres unless noted otherwise.
3. This drawing is to be read in conjunction with the following drawings:
   3350-BAMNU-HAMPS-450-CZ-DR-200004
   3350-BAMNU-HAMPS-450-CZ-DR-200005
   3350-BAMNU-HAMPS-450-CZ-DR-200006

Rev	Date	Issue History
P01.2	2017-09-07	

Description of change - Line 1
Description of change - Line 2
Description of change - Line 3

Description of change for current revision

Checker:
Approver:

P01.2

Work in Progress

Location
Hammersmith Pumping Station
London Borough of Hammersmith and Fulham

Document Information
BMB JV - Lead Designer
Inlet Channel
- Propping sequence

3310-BMBJV-HAMPS-450-CZ-DR-000020
Official

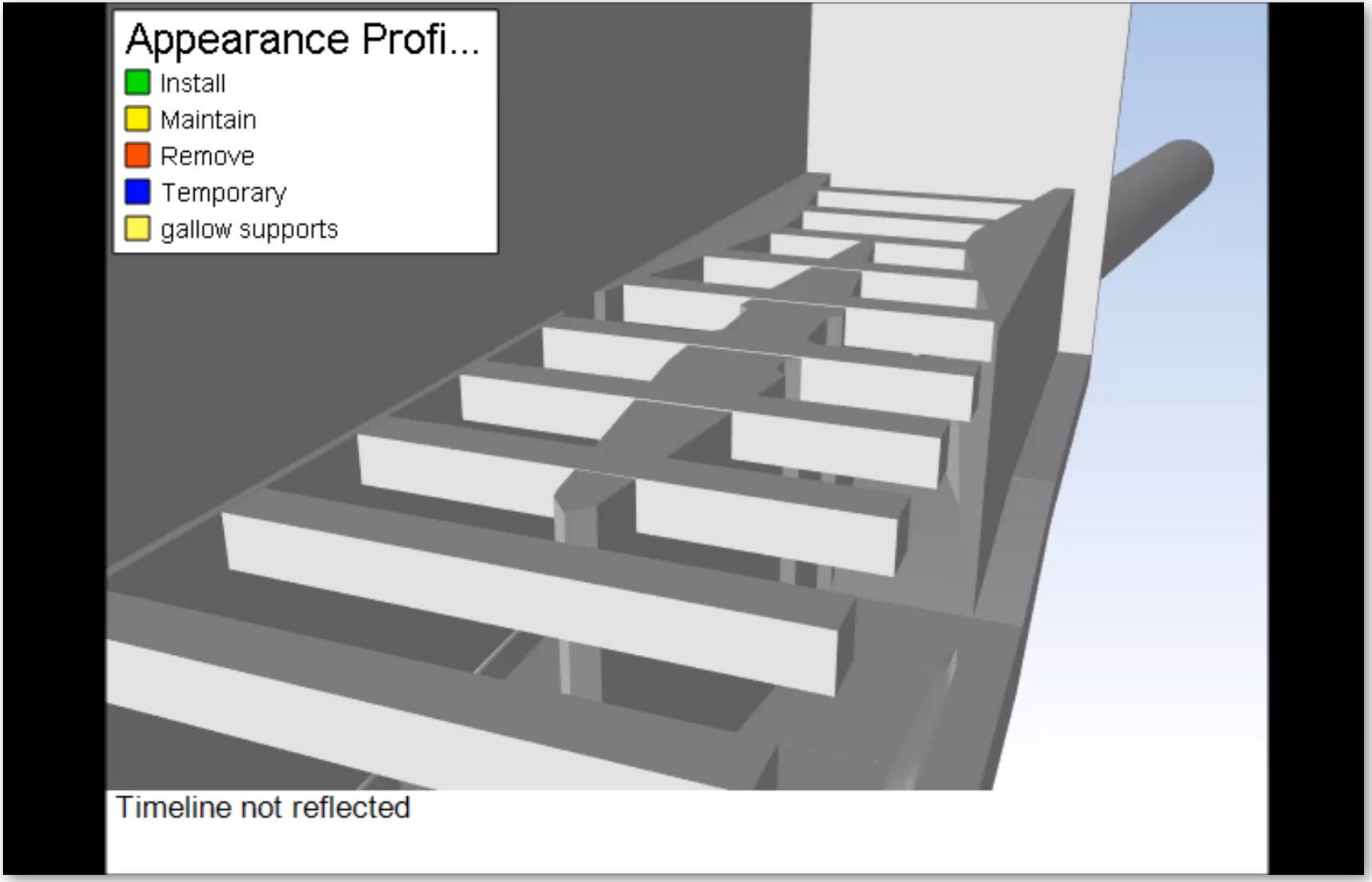
Not For Construction

Tideway

PDF Created: 07/09/2017 12:56:14 Valid only at time of creation

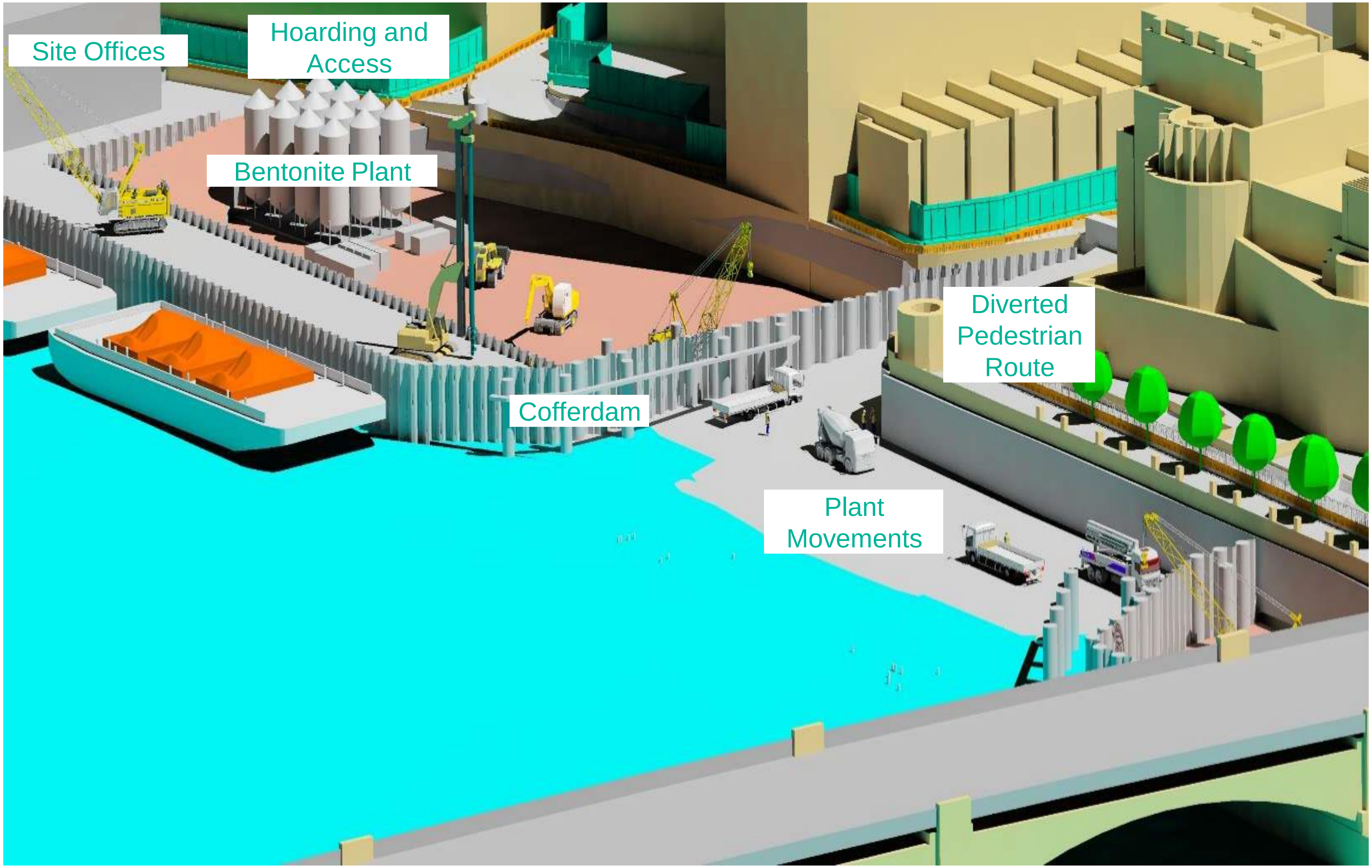
EXAMPLES OF WHERE DIGITAL IS BEING USED

INLET CHANNEL – PROPPING SEQUENCE



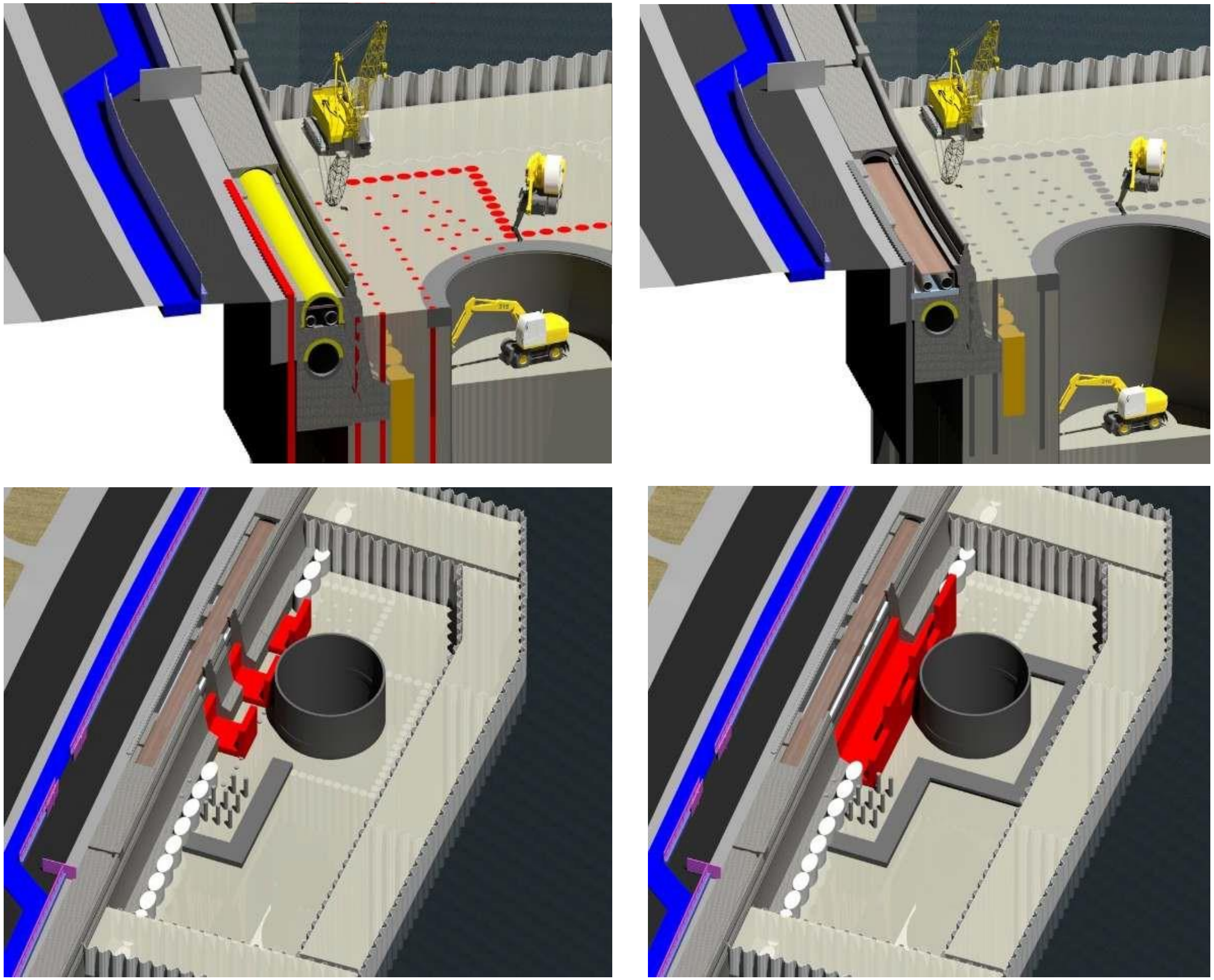
EXAMPLES OF WHERE DIGITAL IS BEING USED

TEMPORARY WORKS AND LOGISTICS MODEL



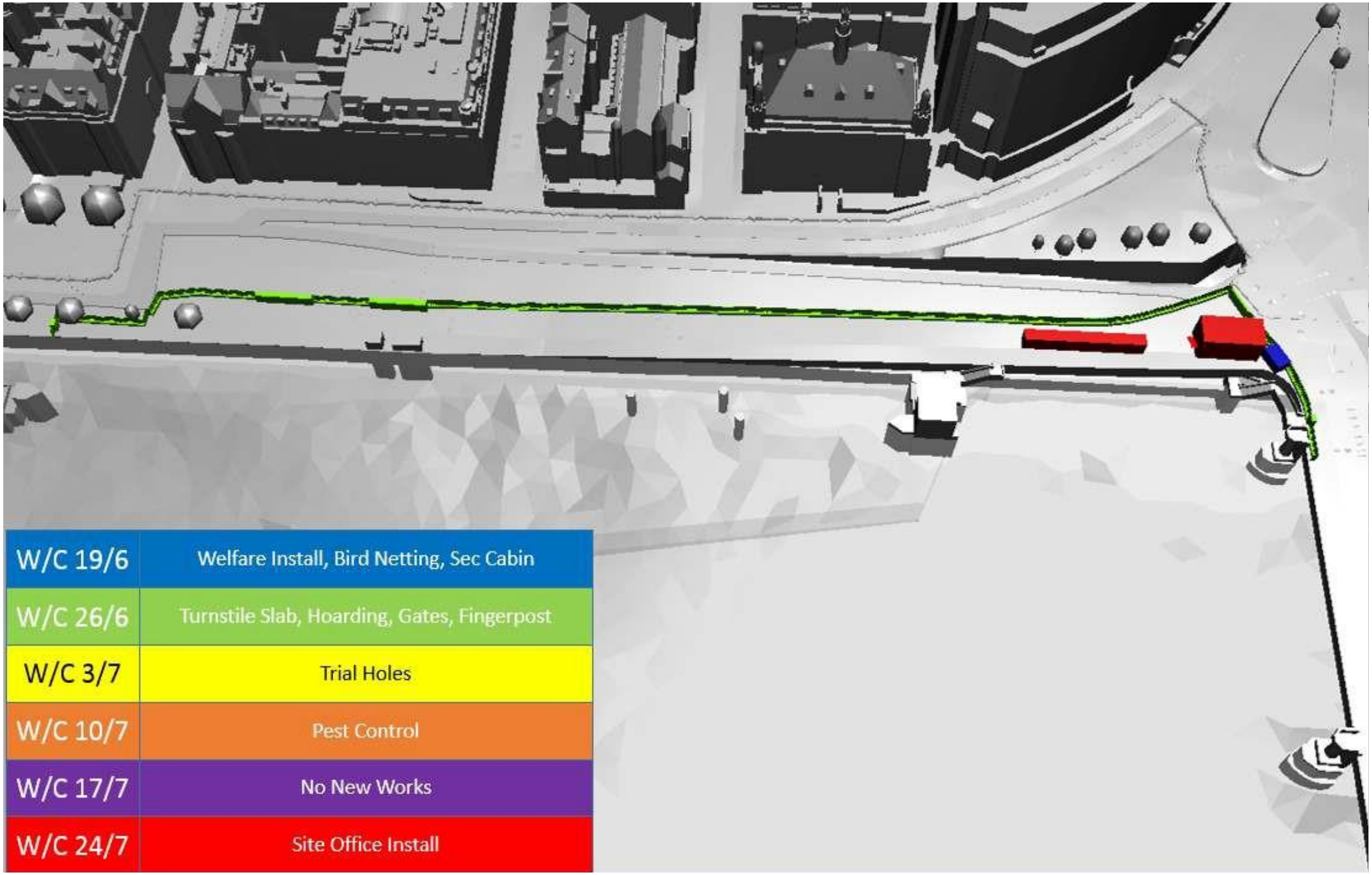
EXAMPLES OF WHERE DIGITAL IS BEING USED

SEQUENCING OF WORKS



EXAMPLES OF WHERE DIGITAL IS BEING USED

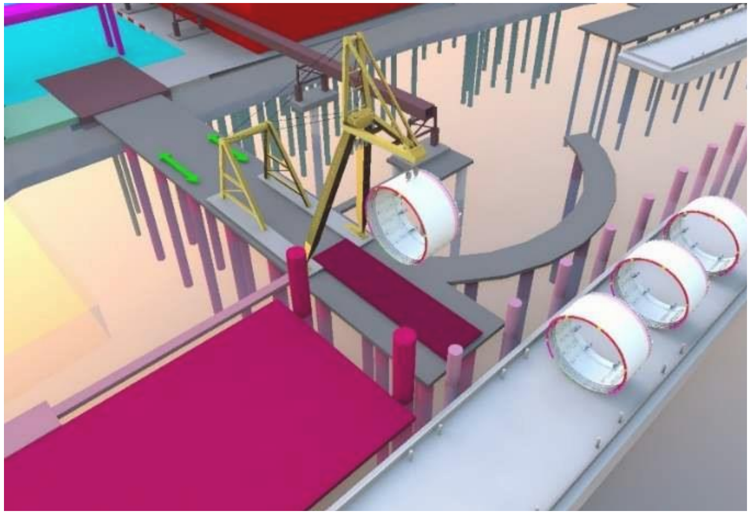
PROGRAMME LOOKAHEADS

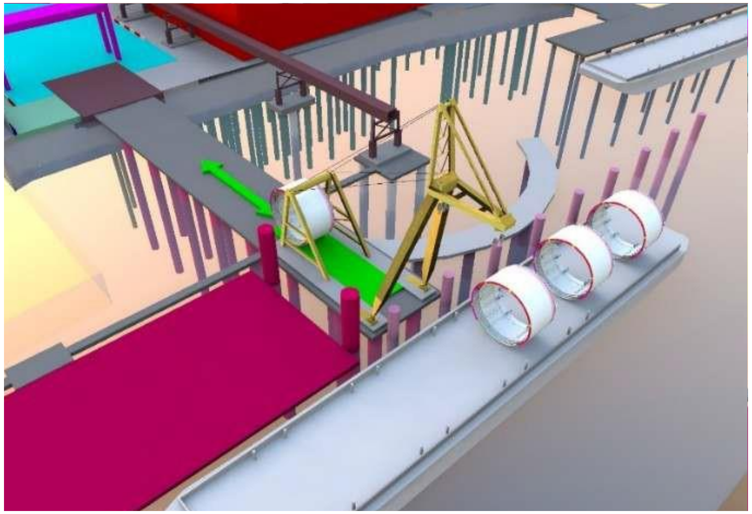


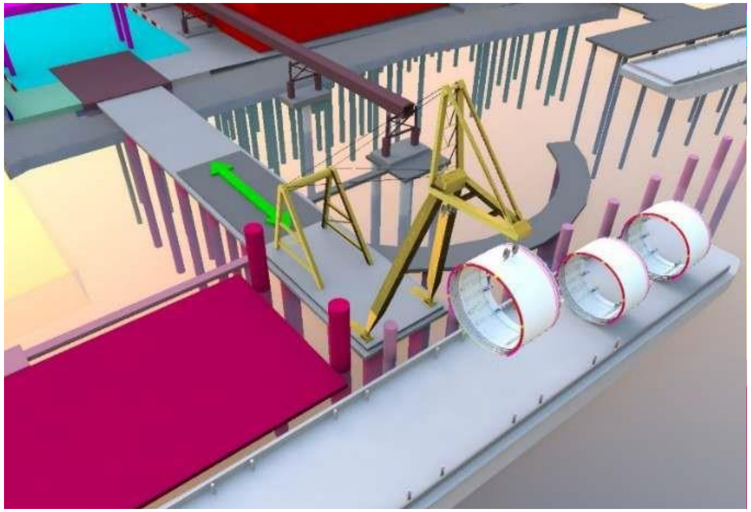
W/C 19/6	Welfare Install, Bird Netting, Sec Cabin
W/C 26/6	Turnstile Slab, Hoarding, Gates, Fingerpost
W/C 3/7	Trial Holes
W/C 10/7	Pest Control
W/C 17/7	No New Works
W/C 24/7	Site Office Install

EXAMPLES OF WHERE DIGITAL IS BEING USED

TBM OPTIONEERING

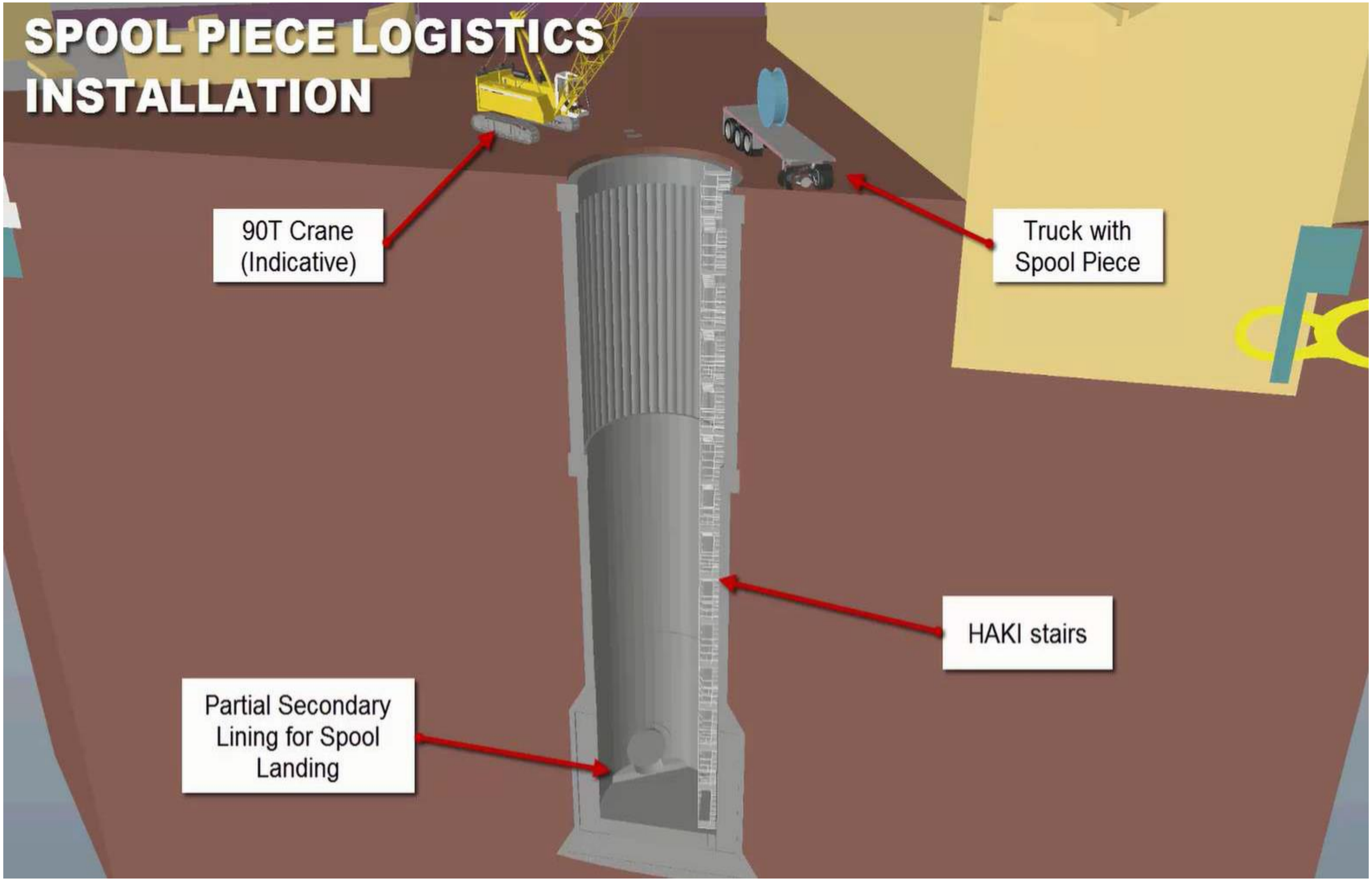






EXAMPLES OF WHERE DIGITAL IS BEING USED

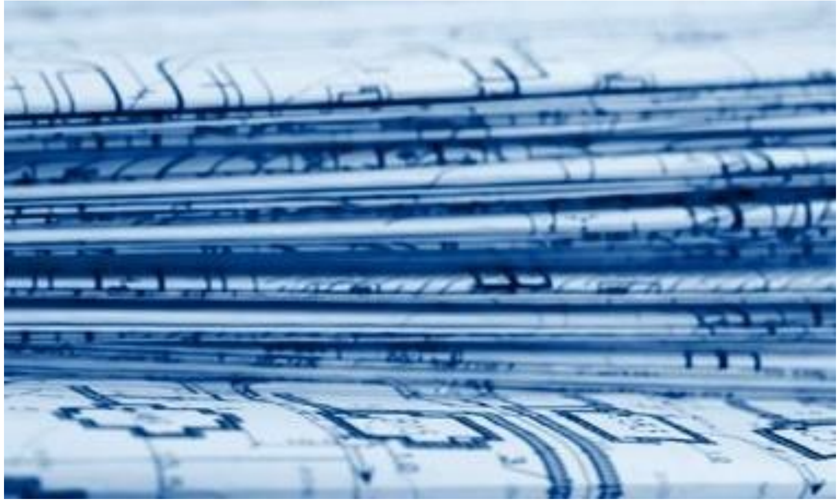
4D – TIME LINKED MODELS

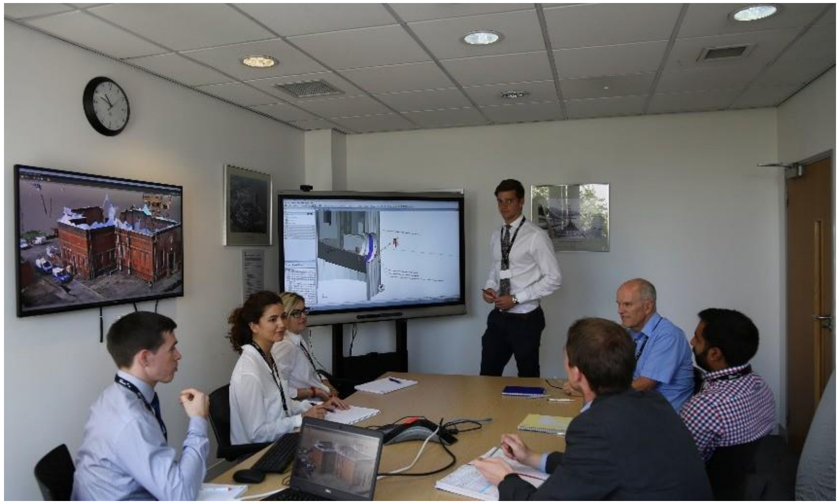


EXAMPLES OF WHERE DIGITAL IS BEING USED

MODEL BASED DELIVERY

- The Challenge
    - Reduce deliverables
    - Reduce programme (more efficient delivery workflow)
    - Build on WI requirement to delivery models
    - Implement BIM at the heart of the project

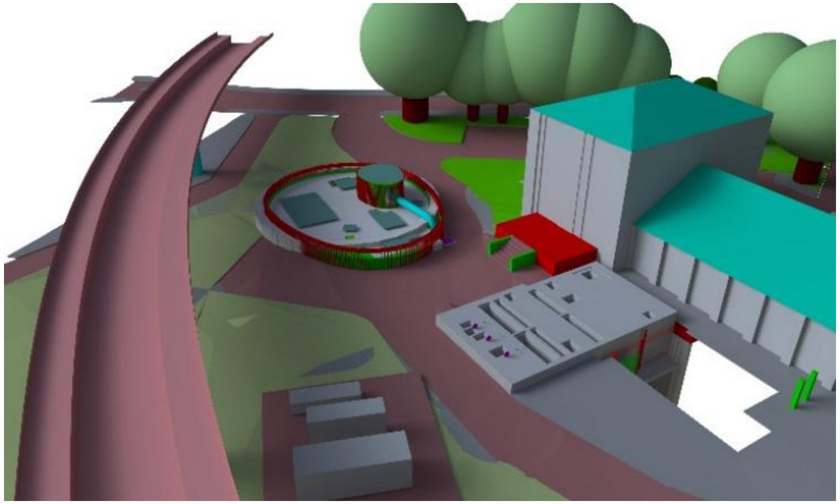


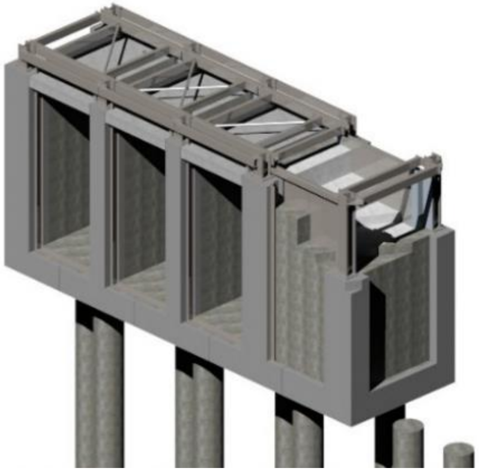


EXAMPLES OF WHERE DIGITAL IS BEING USED

MODEL BASED DELIVERY

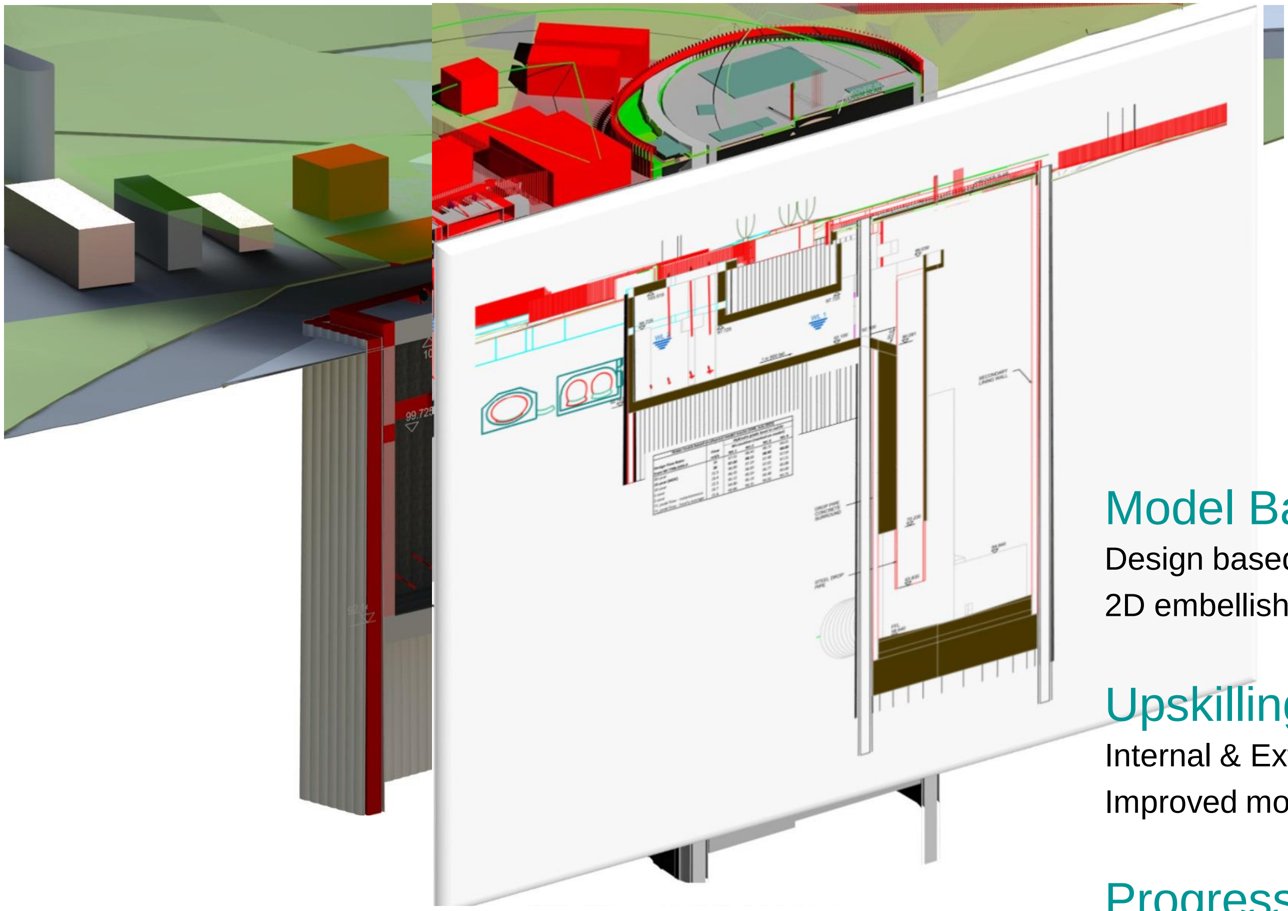
- The Deliverable
  - One single model package per site
  - Reviewed with the contractor weekly
  - Progressive Assurance
  - 2D annotations within the 3D models





EXAMPLES OF WHERE DIGITAL IS BEING USED

MODEL BASED DELIVERY



Model Based Delivery

Design based in the 3D environment

2D embellishments in the 3D model

Upskilling

Internal & External Training Programme

Improved model checking procedures

Progressive Assurance

Weekly collaborative design sessions.

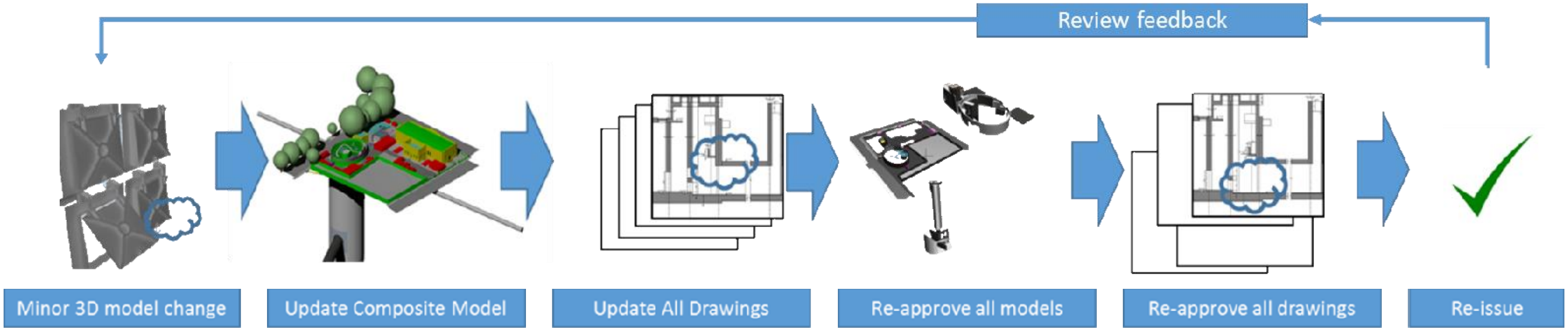
Structured pre-agreed agenda

Open door policy

EXAMPLES OF WHERE DIGITAL IS BEING USED

MODEL BASED DELIVERY

Drawing Based Delivery



Review feedback

Minor 3D model change

Update Composite Model

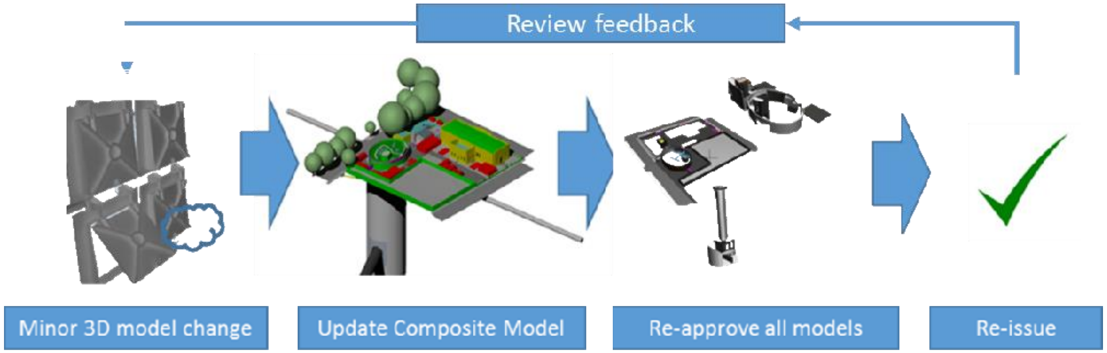
Update All Drawings

Re-approve all models

Re-approve all drawings

Re-issue

Model Based Delivery



Review feedback

Minor 3D model change

Update Composite Model

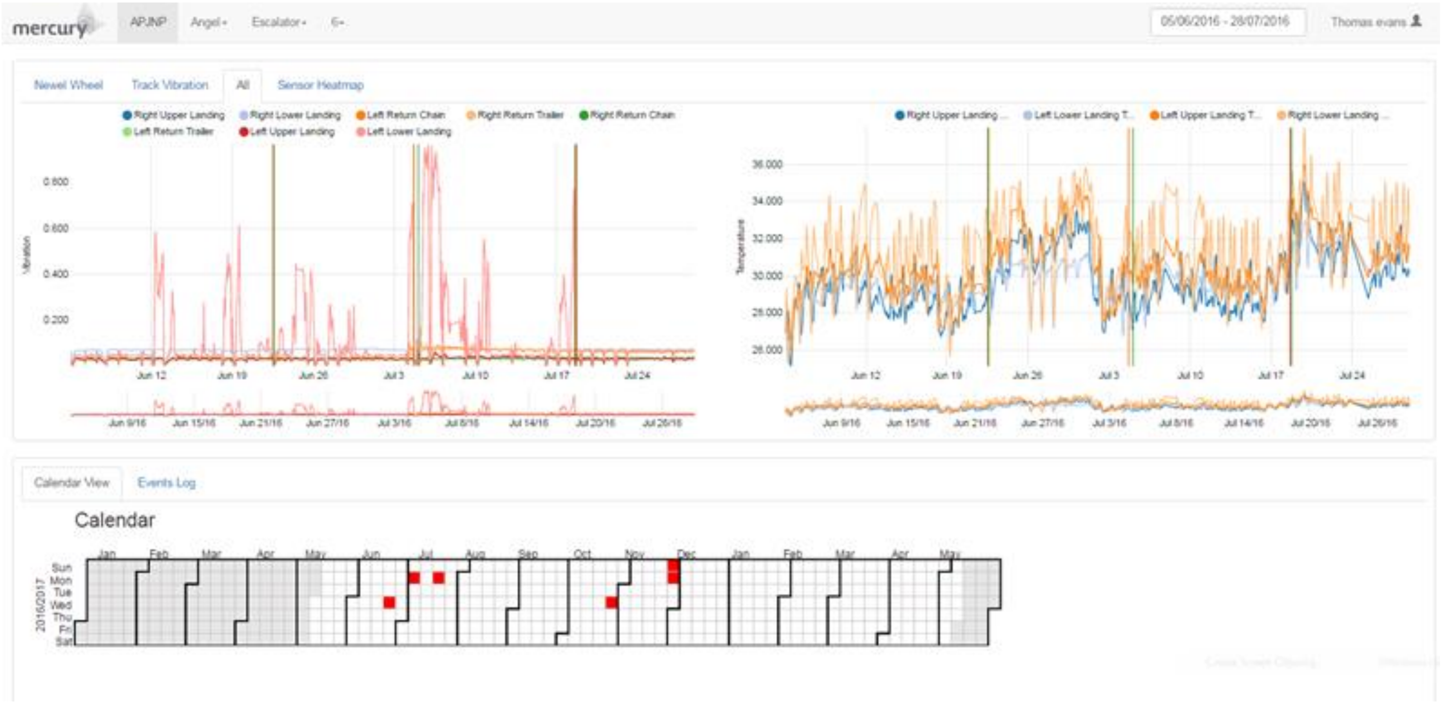
Re-approve all models

Re-issue

EXAMPLES OF WHERE DIGITAL IS BEING USED

SYSTEMS INTEGRATOR (SI)

- The main role of the SI is the development of the SCADA and CSO monitoring systems
- They are using live analytics and artificial intelligence to help monitor assets



EXAMPLES OF WHERE DIGITAL IS BEING USED

SYSTEMS INTEGRATOR

- Monitoring and Prediction
  - Move from asking “What must I do now?” to “What should I do next?”
- Investigation and Diagnostics
  - Machine learning identifies fault fingerprints improving detection rates and lead times, improving asset availability
- Action and Resolution
  - Real time asset information allows investigation of the impact of maintenance

EXAMPLES OF WHERE DIGITAL IS BEING USED

TIDEWAY

WHAT DO WE PROVIDE?

- Consistency
  - Standard information capture across all our delivery partners
  - Compatibility with Thames Water systems
  - Open Data Standards (where possible)
- An eye on the future
  - Ensuring the data we need to operate and maintain the tunnel is collected
- Aggregation
  - Taking data and models from across the project and combining them to get better insights

Tideway

Business Models to Support Digital Innovation

19 September 2017

CONSTRUCTING EXCELLENCE
delivered with bre

Reflection

Introduction

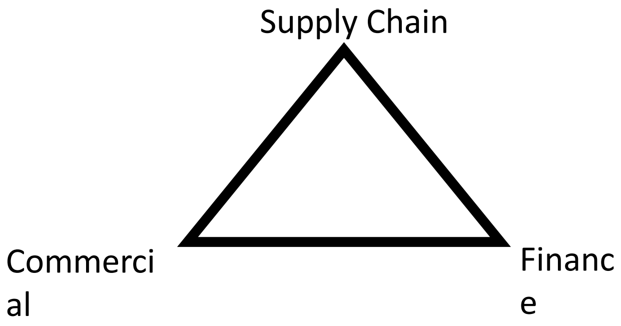
- Transparency & Big Data
- Distributed Ledgers (blockchain)
- Collaboration Map
- Bumps in the Road
- Productivity
- Disruption
- Resilience

Transparency & Big Data

- Open data e.g. self publishing payment terms – subcontractors can choose who to work for
- Open data on Compensation Events. E.g. viewing all CEs across Crossrail to spot themes and trends. What are the most common reasons for change? Prioritise as an industry
- Self policing on fair payment – not relying on legislation
- Step further - has the transaction occurred and were the works 100% complete
- Subcontractor can apply for 110% and try and shame the contractor into paying 100% - risks of new models!
- Asset management regulation

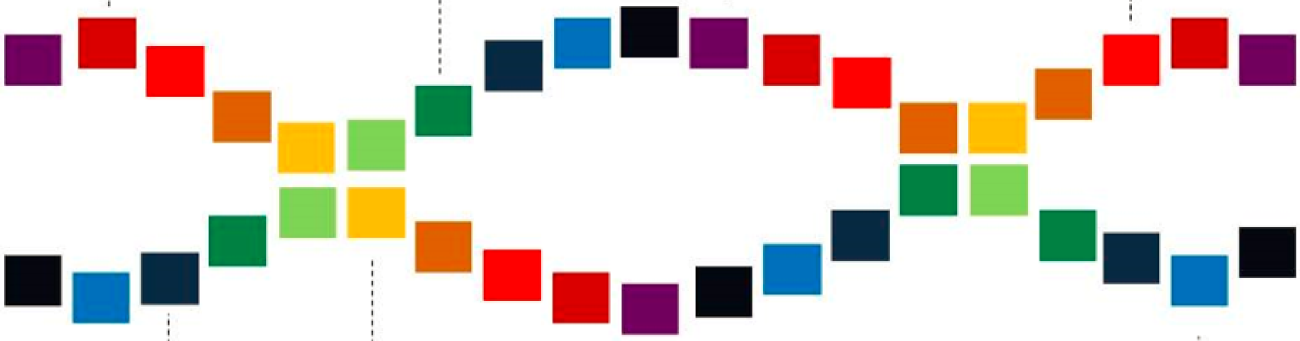
Distributed ledgers (blockchain)

- Fair payment - Pay in a day. Professor David Fisk – pay in 15 minutes
- Existing business models (cashflow; margins)
- Distributed ledgers
- Level 5 BIM - Objectify all elements – codify them – link to Activity Schedule or BoQ (never been done at any kind of scale) Link to payment mechanisms. Commercial – finance – supply chain



- Very admin heavy. Opportunity to link enterprise and project thinking

Mapping a Companies Genome



Corporate Social Responsibility
1 – >2 volunteer days per worker
0 – <2 volunteer days per worker

R&D Investment
1 – ≥5% of turnover
0 – <5% of turnover

Health and Safety
1 – ≤0.07 AFR*
0 – >0.07 AFR*

Payment Terms
1 – Less than 28 days
0 – Over 28 days

Innovation Management
1 – ≥Gold rating
0 – <Gold rating

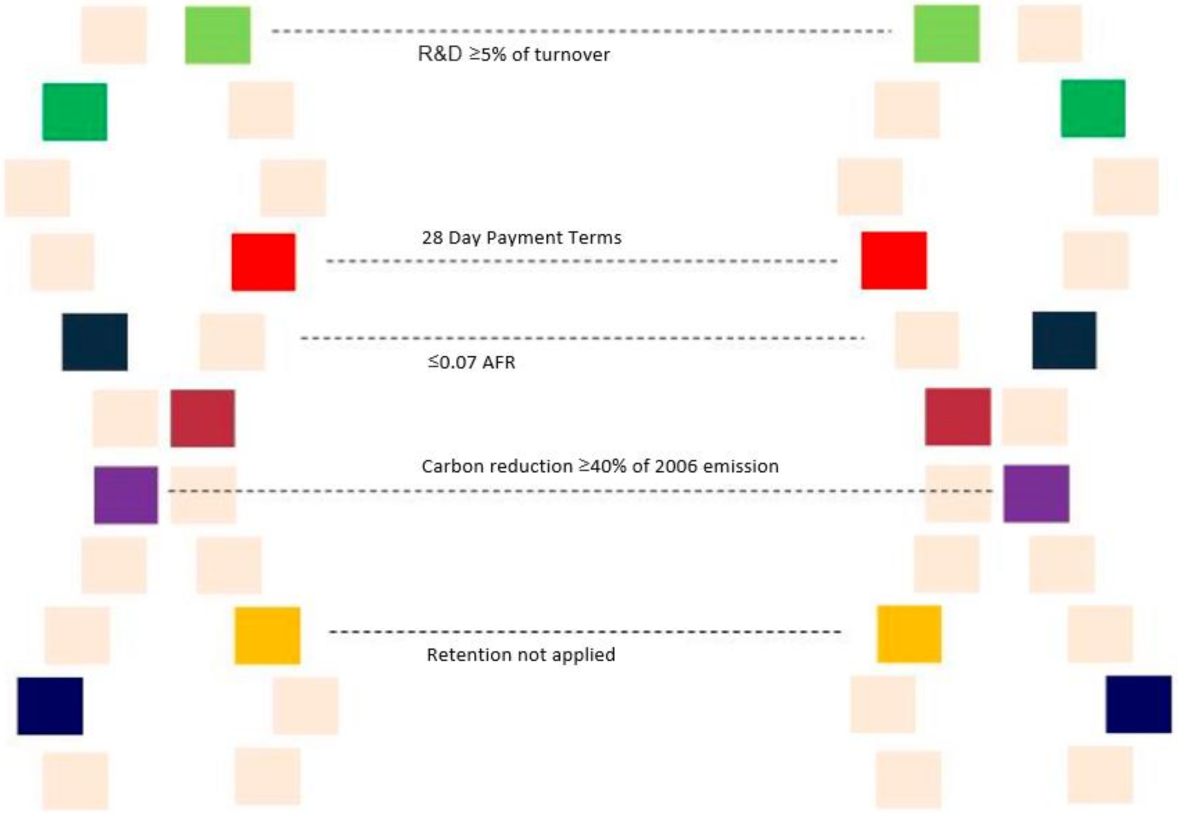
Retention Model
1 – Not applied
0 – Applied

Carbon Reduction
1 – ≥40% of 2006 emission
0 – <40% of 2006 emission

Discounting Model
1 – Early Payment Discount
0 – No Discount

AFR = Accident Frequency Rate

Matching & Discovery of Companies



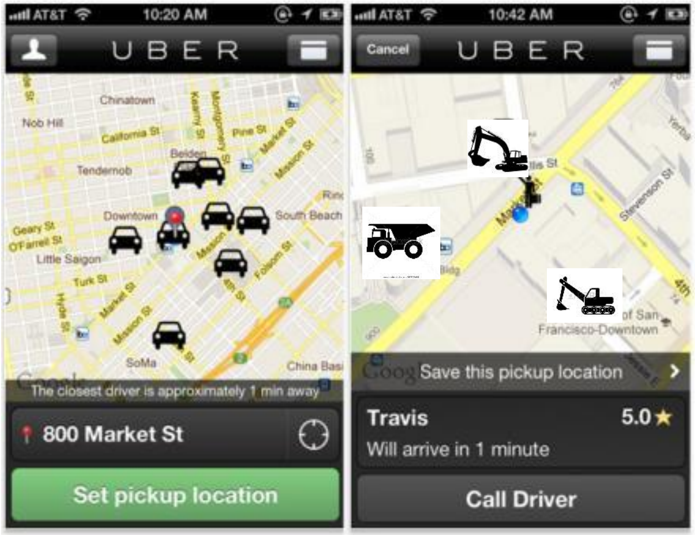
Bumps in the Road

- Trant Engineering Ltd v Mott MacDonald ltd [2017]
- Mid Atlantic Power Project
- £55m power station in the Falkland Islands
- Mott MacDonald was appointed to provide design services and was also the BIM coordinator, controlling access to the common data environment (CDE)
- Trant was entitled to have access to the design data which had already been placed in shared folders

Productivity

- Innovation will always beat productivity
- Less administration (contract and admin)
- Productivity and automation. Skills gap – how we deliver projects will fundamentally change
- Manufacturing – Offsite construction is arguably doing what we do now but indoors. Manufacturing processes will involve an assembly line approach to delivering better quality products
- Designers not encouraged to standardise. Billable hours

Productivity



The closest driver is approximately 1 min away

Travis 5.0 ★

Will arrive in 1 minute

- Under utilised resource – Uber for plant
- Find your required plant based on locality (using GPS)
- Find you required plant based on specification and certification
- Compare prices of the plant from different plant providers
- Select plant based upon previous user feedback and ‘likes’
- Get the plant delivered upon request; or go and collect it yourself
- Handle the payment and administration via by an application
- This is being done now in the USA – Getable

Disruption

Elon Musk

@elonmusk

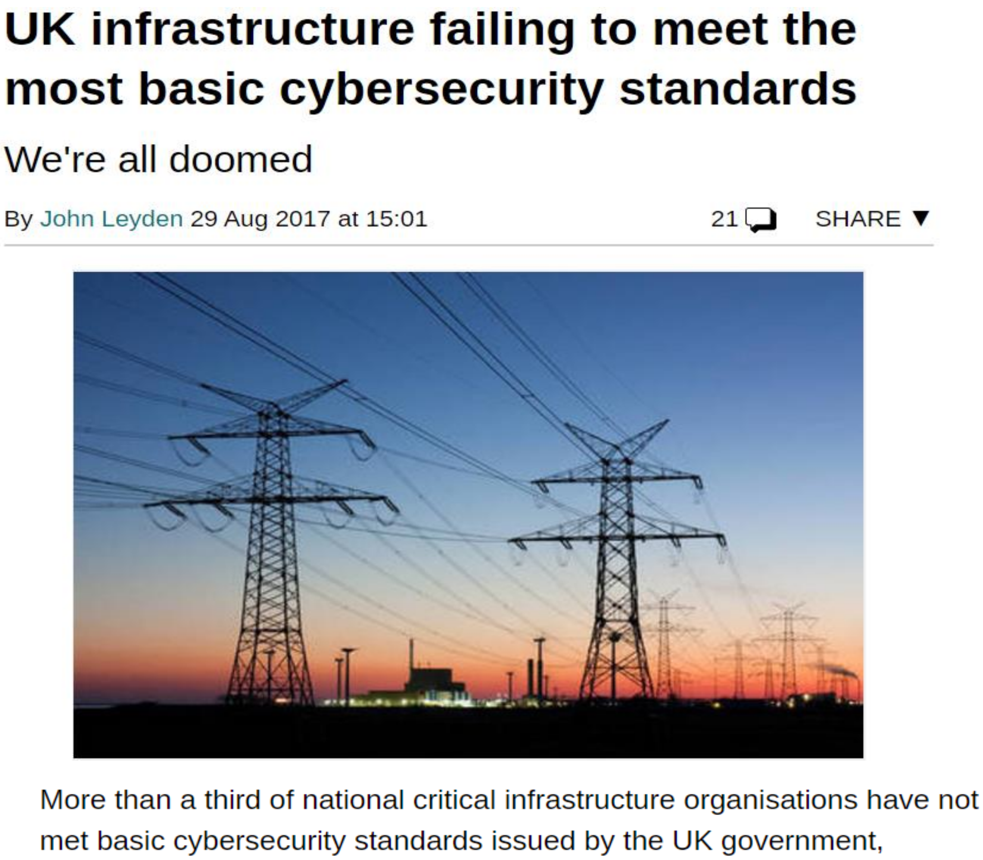
Tesla, SpaceX, Tunnels & OpenAI

1 AU

Joined June 2009

“We’re just going to figure out what it takes to improve tunnelling speed by, I think, somewhere between 500 and 1,000 percent”

Resilience



UK infrastructure failing to meet the most basic cybersecurity standards

We're all doomed

By John Leyden 29 Aug 2017 at 15:01

21 SHARE ▼

More than a third of national critical infrastructure organisations have not met basic cybersecurity standards issued by the UK government,

Summary

- Commissioners may begin to work directly with disruptors
- Payment methods and incentives will change
- Cyber risk must be taken seriously and programmed in
- Must ensure that data is treated as a major asset