

Digital Twins: An analysis framework

Hugh Boyes CEng FIET CISSP

Principal Engineer, WMG Cyber Security Centre



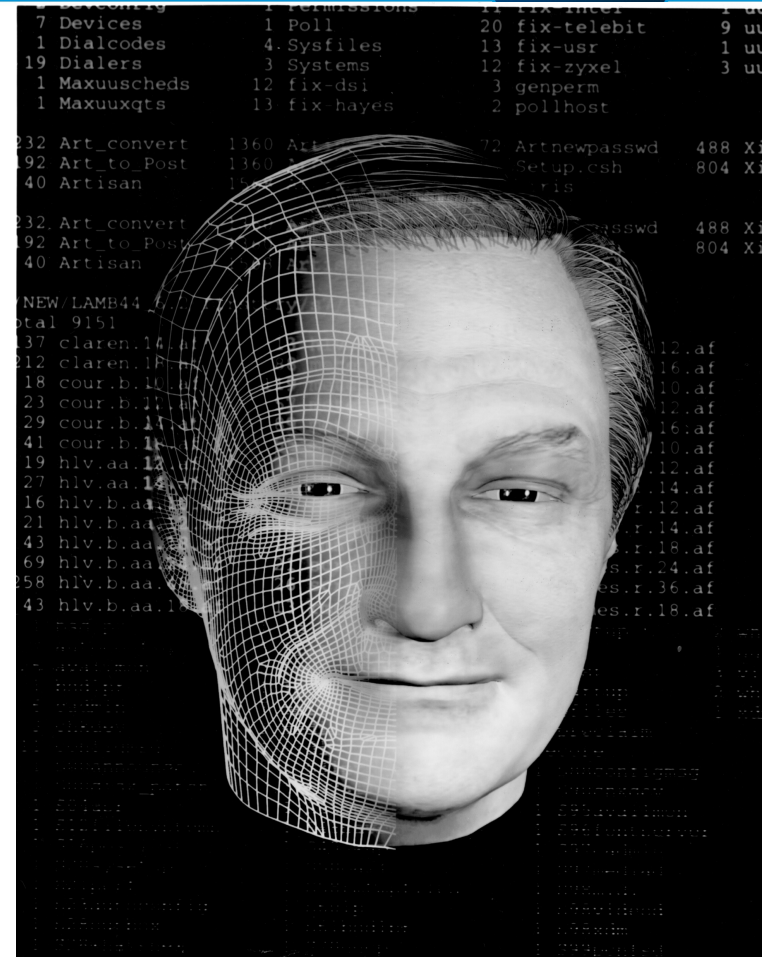
Digital Twins

Background & Definitions

First Digital Twin

Scientific American Frontiers: “The Art of Science”
broadcast !8TH February 1998

Picture of a preliminary stage in the creation of “Alan 2.0,”
a digital twin of Alan Alda. Said to mark the first time a
real-life person had been assembled digitally from images
and voice fragments.



Terminology

Digital model

Digital shadow

Digital twin

Computational models of
physical assets or processes
or systems)

NASA (2010)

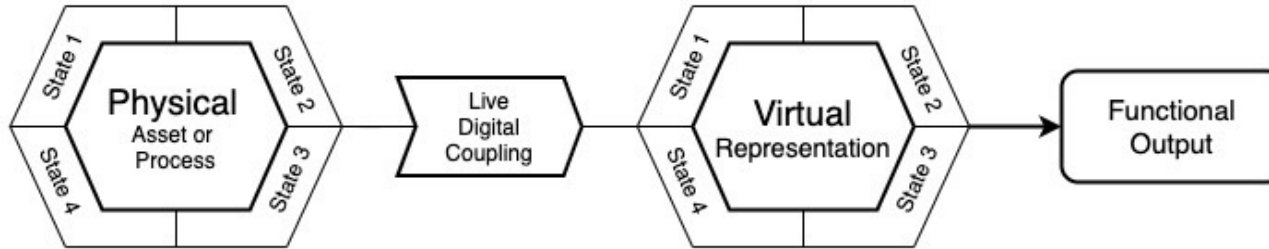
*“Digital twin - an integrated **multi-physics**, multi-scale, probabilistic simulation of a vehicle or system that uses the best available **physical models**, sensor updates, fleet history, etc., to mirror the life of its flying twin”*

<https://www.gov.uk/government/publications/computational-modelling-blackett-review>

<http://dx.doi.org/10.1098/rsos.172096> [Computational modelling for decision-making: where, why, what, who and how]



A manufacturing digital twin vision

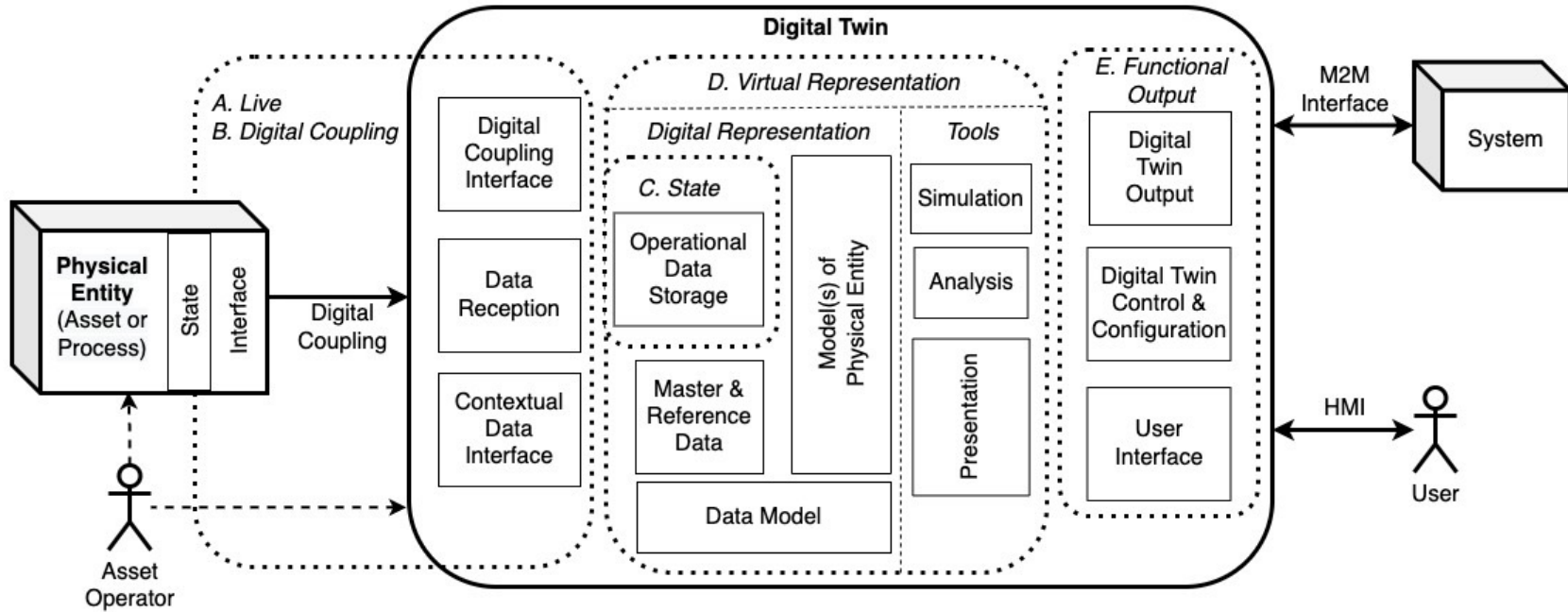


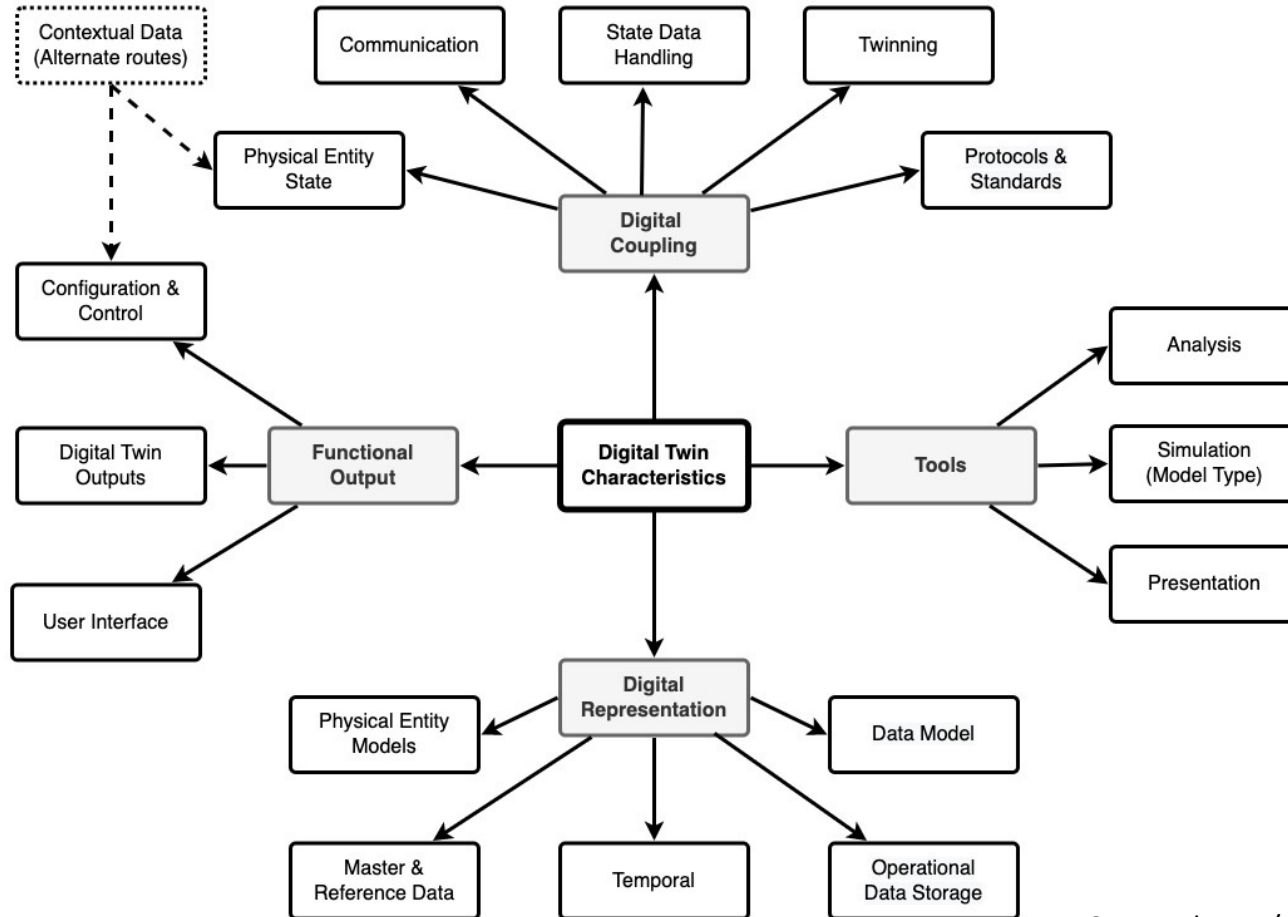
Component	Definition
Live	the state information is available in a timeframe that is close enough to the underlying event
Digital coupling	the transmission mechanism between data source(s) and data consumption method(s) using a digital carrier medium
State	the particular condition the unique physical asset or process is in at a specific time
Physical asset or process	an entity with an existence that has economic, social or commercial value.
Virtual representation	an analogous description or logical model to its physical asset or process
Functional output	information transmitted to a system or human observer that is actionable to deliver value



Digital Twin: Functional composition

Functional composition - example





Digital Twin Characteristics

(Top-level view)

Security and a Digital Twin

Security and Digital Twins

Physical Twin (PT)

- ▶ Inaccurately represented in DT
- ▶ DT used for hostile reconnaissance
- ▶ Unauthorised access to DT leads to malicious acts against PT
- ▶ Sensor failure misrepresents state of PT or its environment

Digital Twin (DT)

- ▶ Inaccurately records configuration/composition of PT
- ▶ Permits unauthorised changes to PT
- ▶ Inaccurately displays state of PT
- ▶ Exposes sensitive intellectual property

Security affected by scope of Digital Twin & required functionality

Developing holistic security view

Security Domains

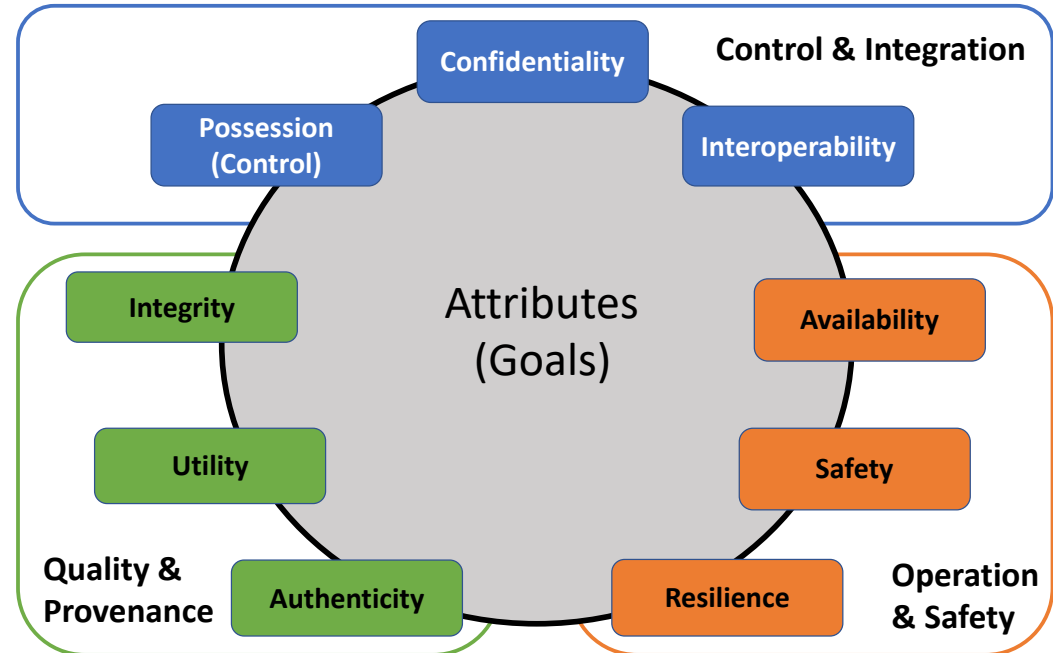
Physical
security

Personnel
security

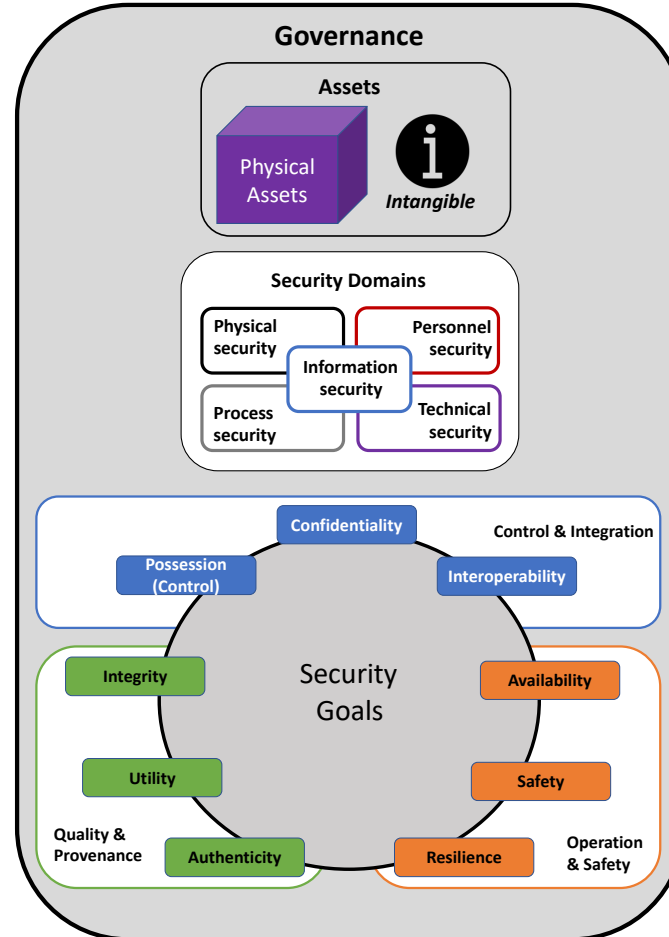
Information
security

Process
security

Technical
security



A holistic view of security for cyber-physical systems



Questions

Hugh Boyes
hb@warwick.ac.uk
hugh.boyes@bodvoc.com

Appendix

Developing a Digital Twin Use Case

Developing a digital twin use case

Structured 4 stage process - 20 questions:



- A. Identify the need
- B. Establish data and/or information requirements
- C. Define information management requirements
- D. Define security requirements

A. Identify the need

1. What outcomes are you seeking to achieve using a digital twin?
2. Are there alternative ways of achieving the outcome without using a digital twin?
3. What is the physical scope covered by the digital twin?
4. Do you own and/or operate all the assets covered within the digital twin's scope?
5. What decisions do you need to make, and/or tasks you will perform using the digital twin?
6. What data and/or information do you need to inform the decisions and/or complete the tasks?

B. Establish data/information requirements

7. For the assets in scope of the digital twin, what is the required granularity of the composition, characteristics, connectivity, behaviour, performance and associated processes?
8. How will you source and maintain this data and/or information?
9. How will the composition, behaviour and operation of the assets be modelled?
10. Is any of the data and/or information received, processed or displayed by the digital twin sensitive?
11. Who will need access to the data and/or information?
12. Who should not have access to the data and/or information?

C. Define information management requirements

13. What are the required quality characteristics of the digital twin?
14. What are the provenance requirements for the models and/or algorithms supporting it?
15. What lifecycle of the digital twin and how will it be managed, and by whom?
16. What are the governance arrangements for the digital twin?
17. Where is the data and/or information used by the digital twin stored and processed?

D. Define security requirements

18. What are the security implications of unauthorised access to or use of the digital twin?
19. What are the privacy implications of unauthorised access to or use of the digital twin?
20. What is the security strategy for the digital twin?

Hugh Boyes
hb@warwick.ac.uk
hugh.boyes@bodvoc.com

