Security and Privacy of Digital Twins - Workshop

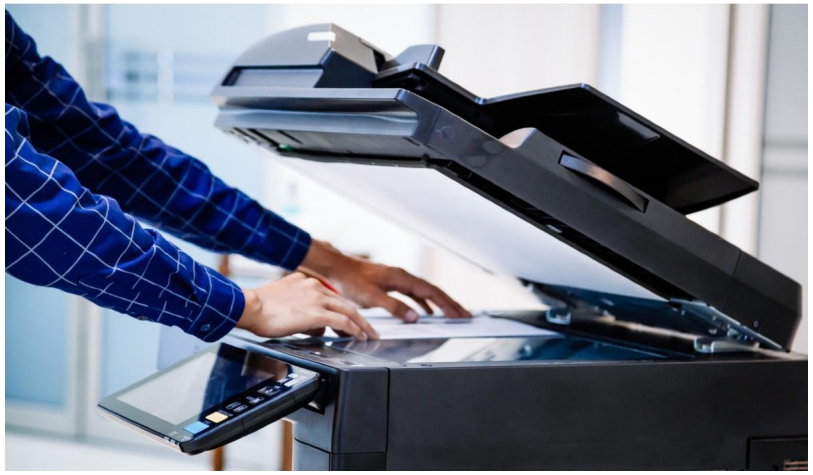
Karim Tobich, Dr.

CyberSecurity & Technology Consultancy

Digitalisation

Physical document

Scanner



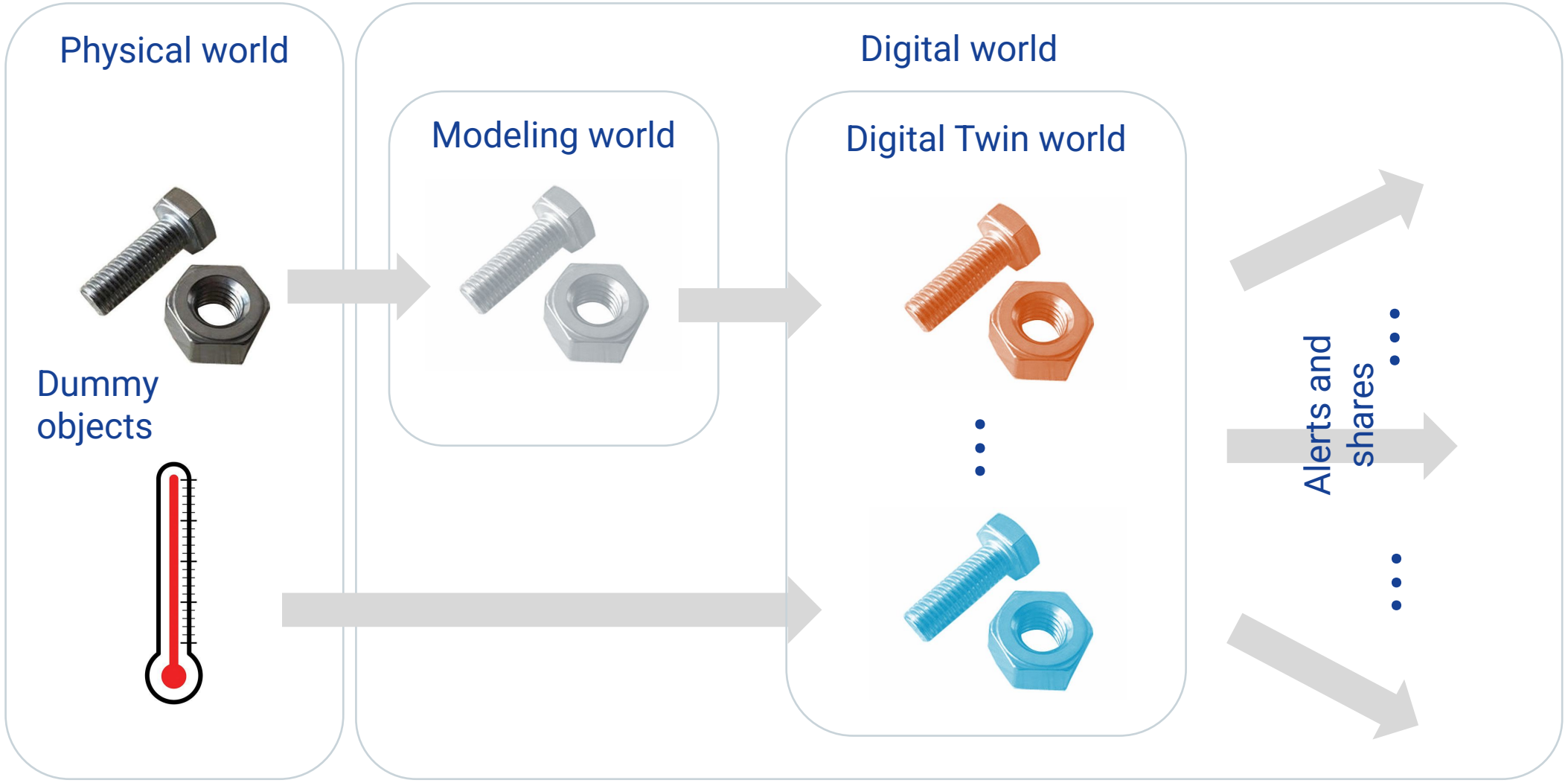
digital document

Does it make it a digital twin?

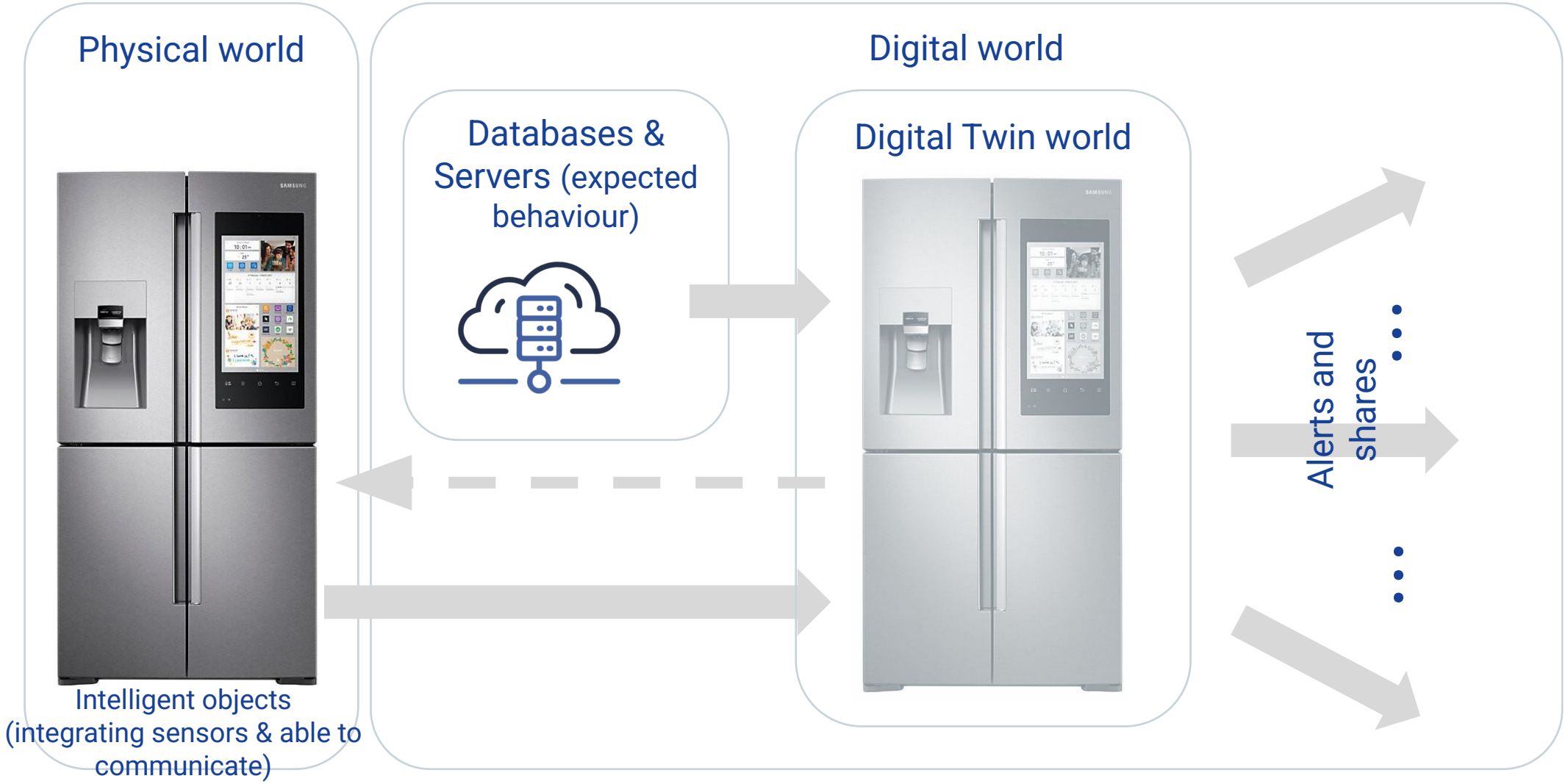
Mirrored Spaces Model (Twin model)

Since its creation NASA was using redundancy within their design and even mirrored modules (models): one module in space and a copy on Earth. Does it make it a digital twin?

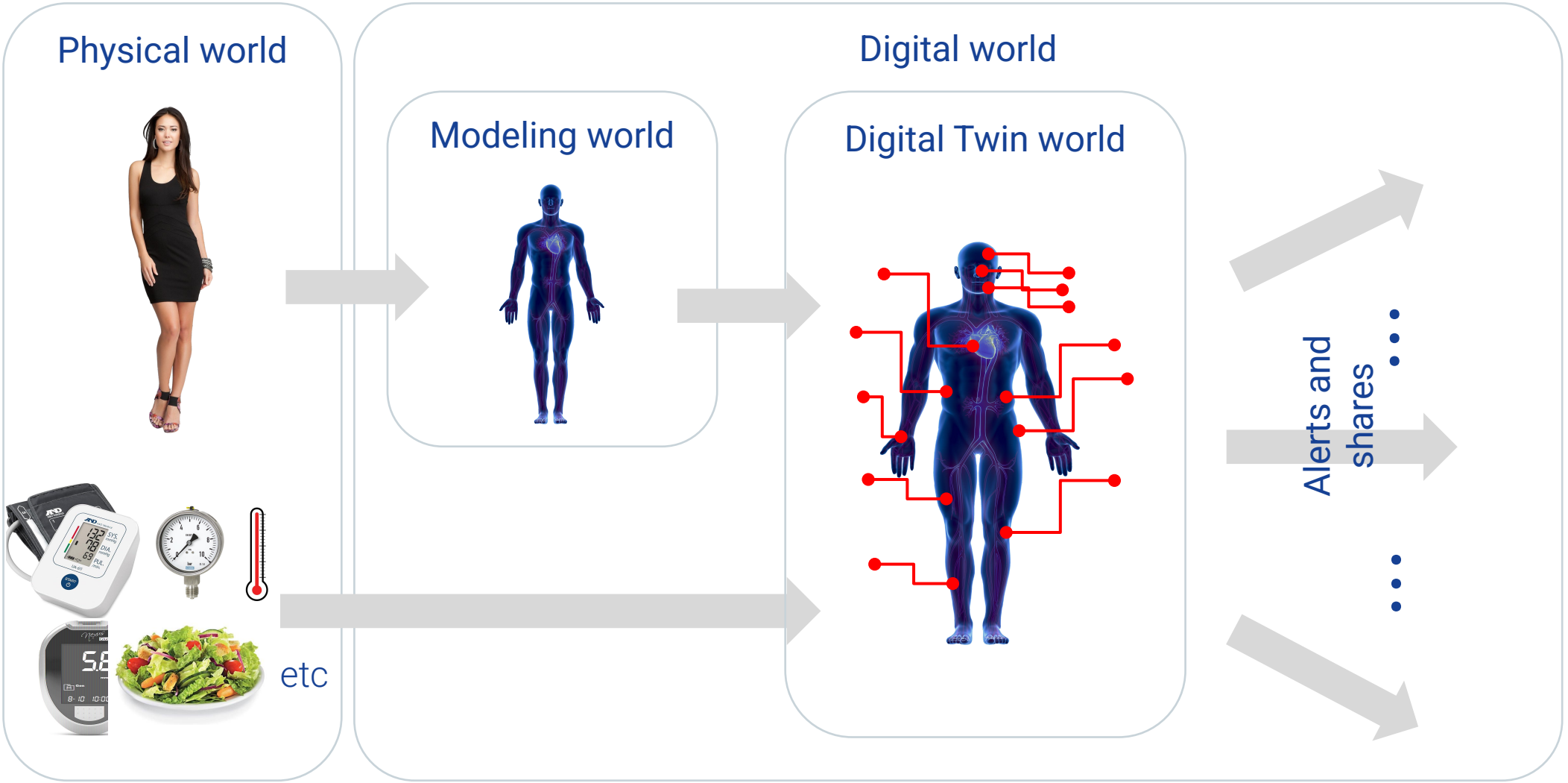
Example



Example



Example



Definitions

Digital Twin (DTw): ***Digital representation*** of a ***target entity*** with data connections that enable convergence between the physical and digital states at an appropriate rate of synchronization.

Note 1 to entry: Digital twin has some or all of the capabilities of connection, integration, analysis, simulation, visualization, optimization, collaboration, etc.

Note 2 to entry: Digital twin can provide an integrated view throughout the life cycle of the target entity.

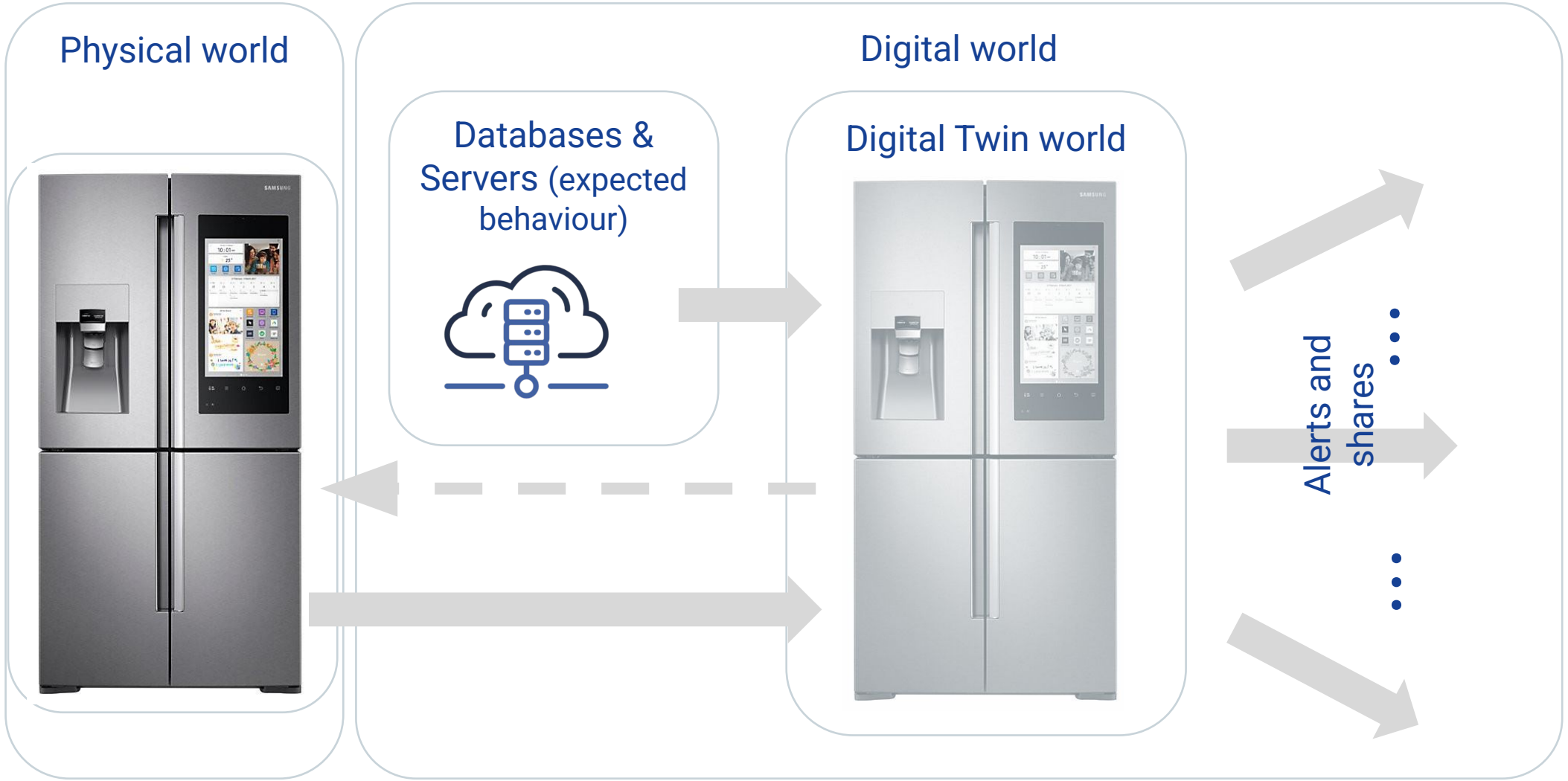
Digital representation: Digital entity representing either a set of properties or behaviours or both of one or more observable elements.

target entity: Entity providing a functional purpose in reality which is the subject of digital representation
Note 1 to entry: The target entity, which provides some functional purpose in reality, can be either physical or digital under consideration.

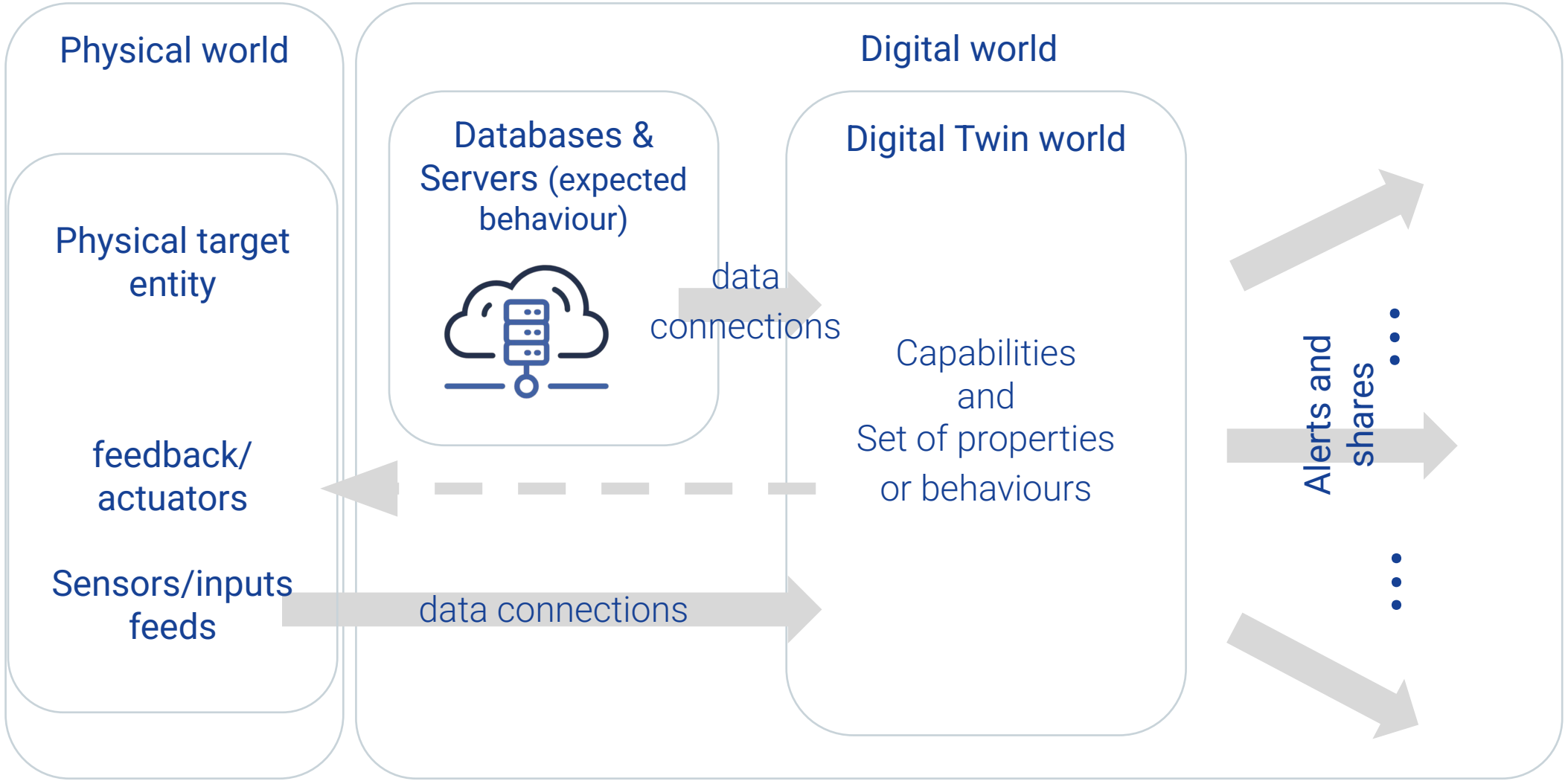
For more details ISO/IEC 30173 Digital twin - Concepts and terminology https://webstore.iec.ch/en/publication/68081

CyberSecurity & Technology Consultancy

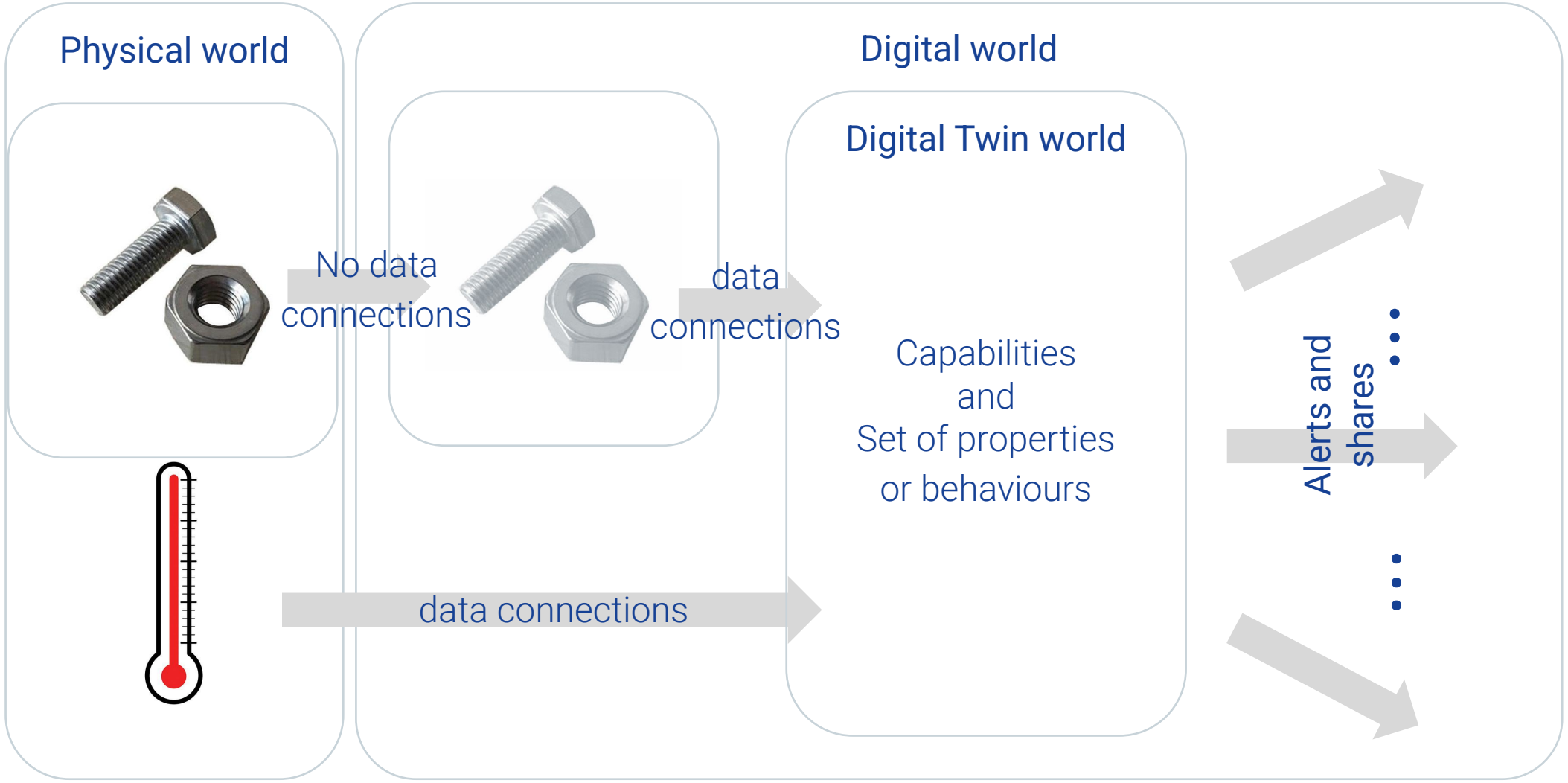
Definitions mapping



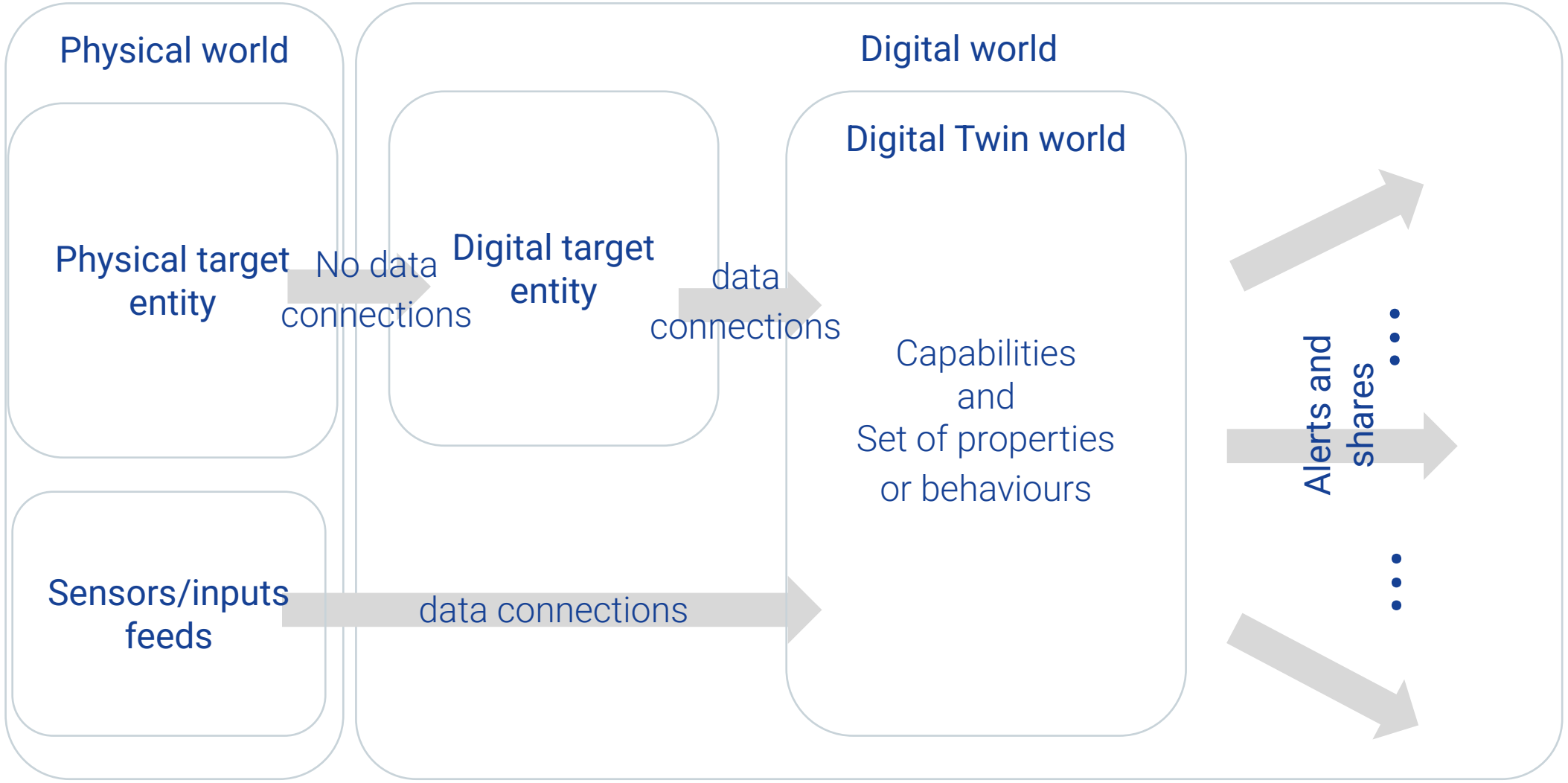
Definitions mapping



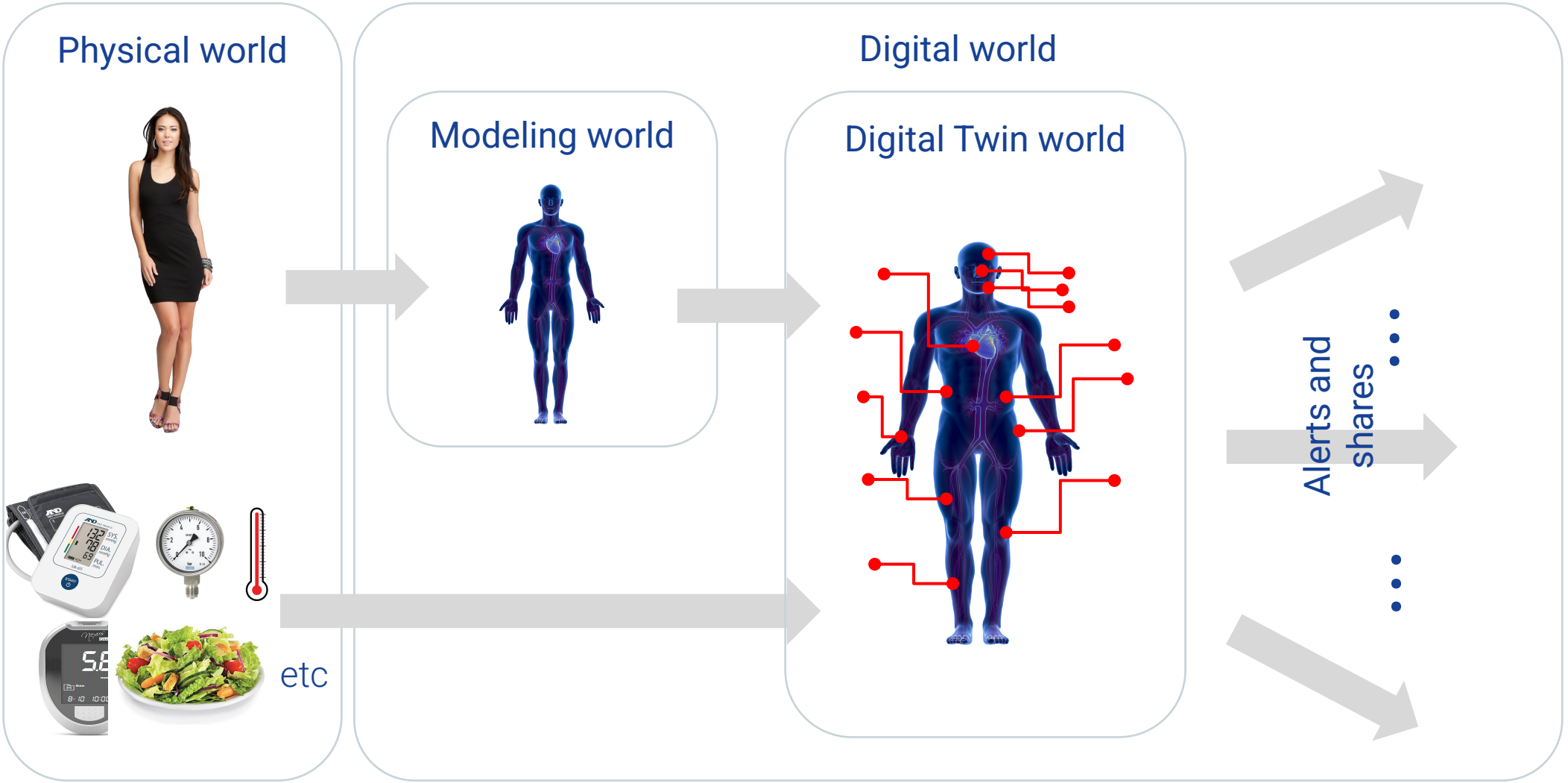
Definitions mapping



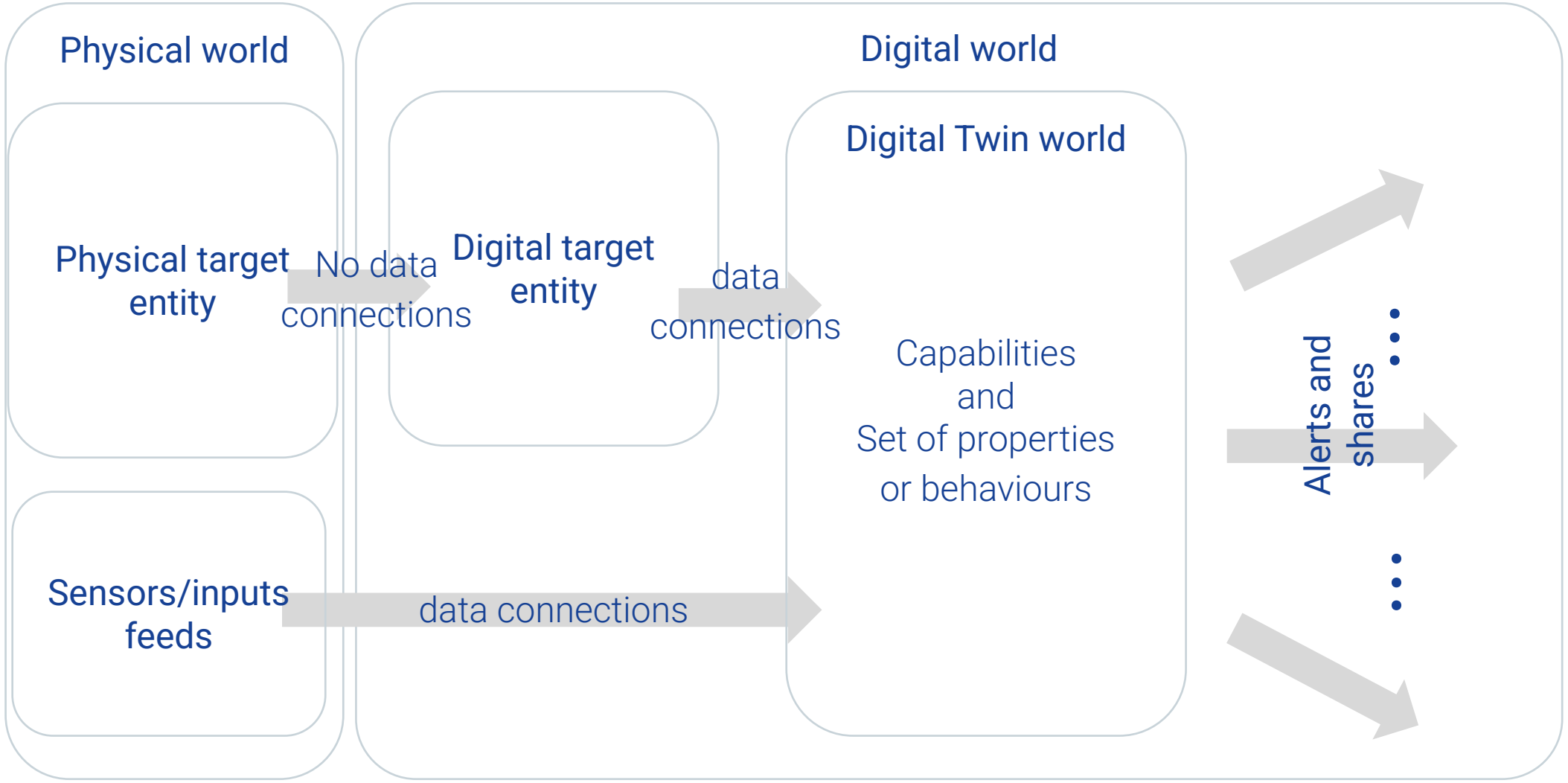
Definitions mapping



Example



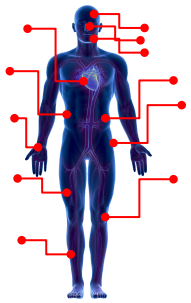
Definitions mapping

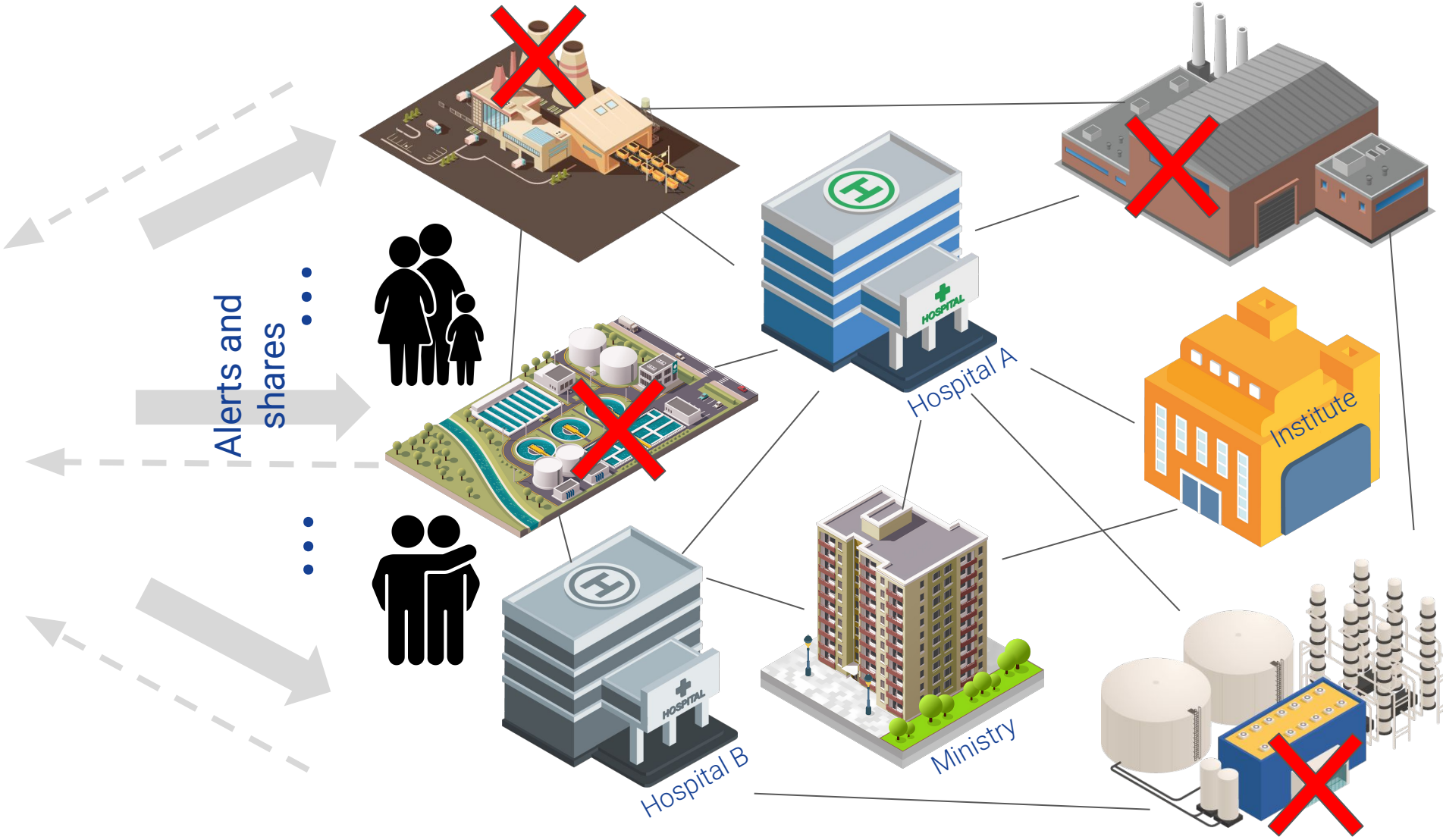


Alerts and shares

Digital Twin world

Capabilities
and
Set of properties
or behaviours

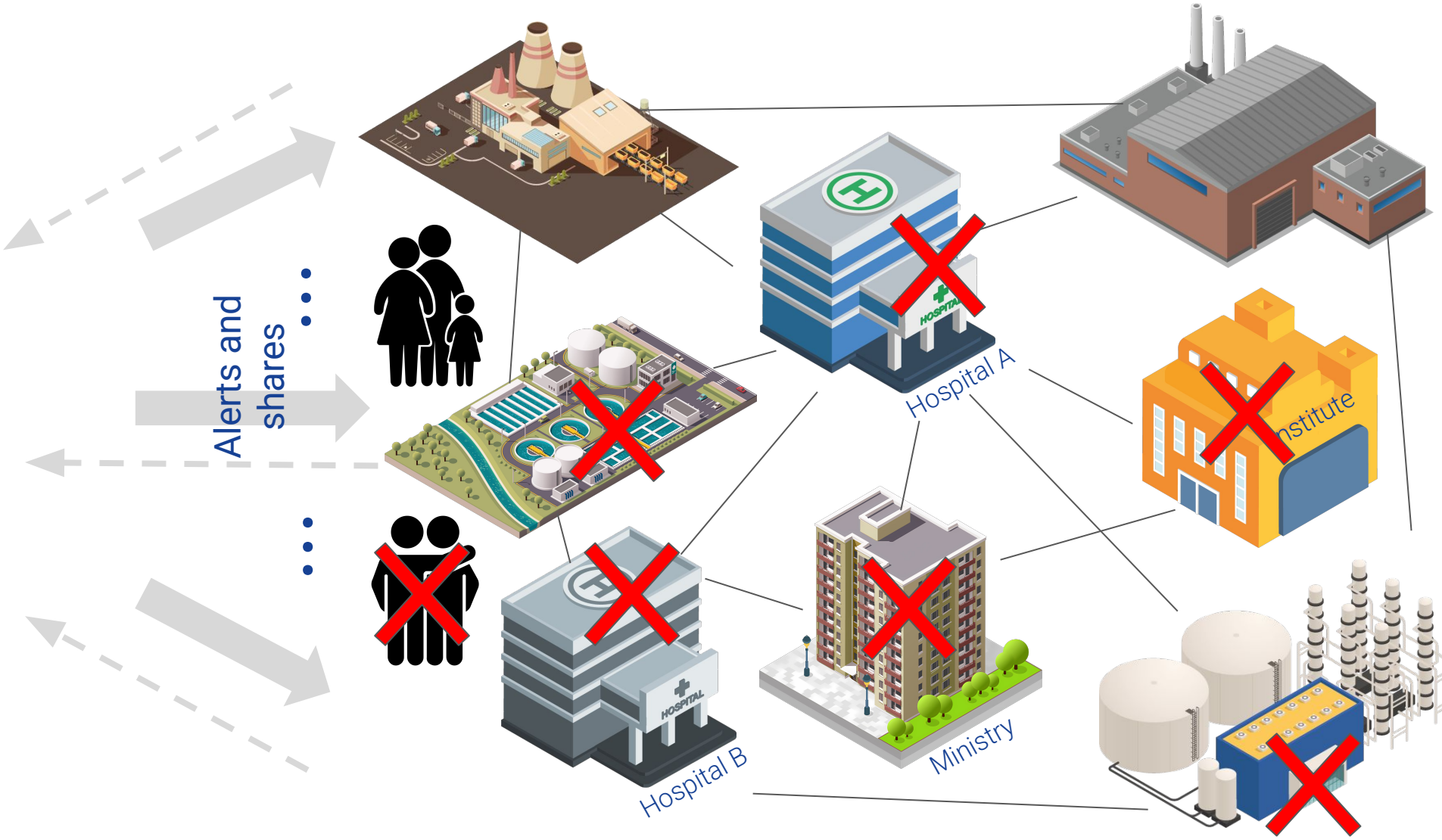




Alerts and shares

Digital Twin world

Capabilities
and
Set of properties
or behaviours



Life cycle and supply chain

Physical world

data connections

etc

Digital twin world

Manufacturer's databases & Servers (simulation)

Airport & civil aviation authority Monitoring system

Airline's databases & Servers (maintenance)

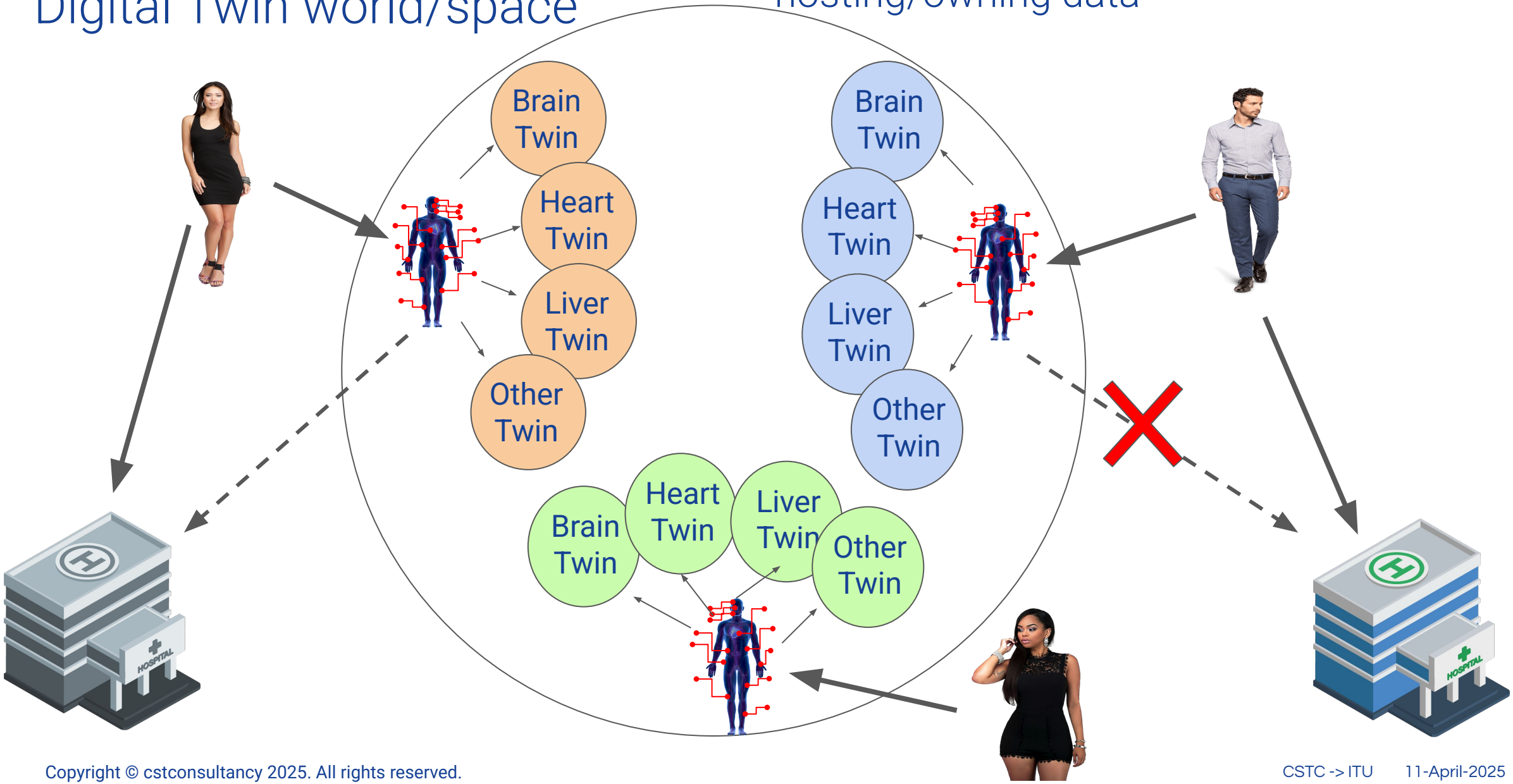
- Easy to share data with supply chain (selective share)
- Easy to investigate & maintain
- Highly secure & safe
- Almost instantaneous response

Incident → Pilot analysis → Airport investigation → Airline investigation → Manufacturer investigation

CyberSecurity & Technology Consultancy

Digital Twin world/space

Private company hosting/owning data



Security & Privacy risks

- Inner risks related to the physical entity:
  - Entity malfunctioning or hacked, sensor or actuator feeding inaccurate data, not appropriate frequency of synchronization (DoS, DDoS attacks of the physical entity),

- Inner risks related to the digital entity:
  - Entity hacked, the feed of data is inaccurate, model incorrect, not appropriate frequency of synchronization (DoS, DDoS attacks of the digital entity),

- Inner risks related to the digital twin:
  - Risks related to the ownership of the data,
  - Risks related to the data storage - unencrypted or insecure storage,
  - Risks related to the data segregation - access to one shared environment,
  - Risks related to the the type of data,
    - biological and health data,
    - personal data,
    - proprietary data,
    - community data,
    - Consortium data,
    - Public data

Security & Privacy risks

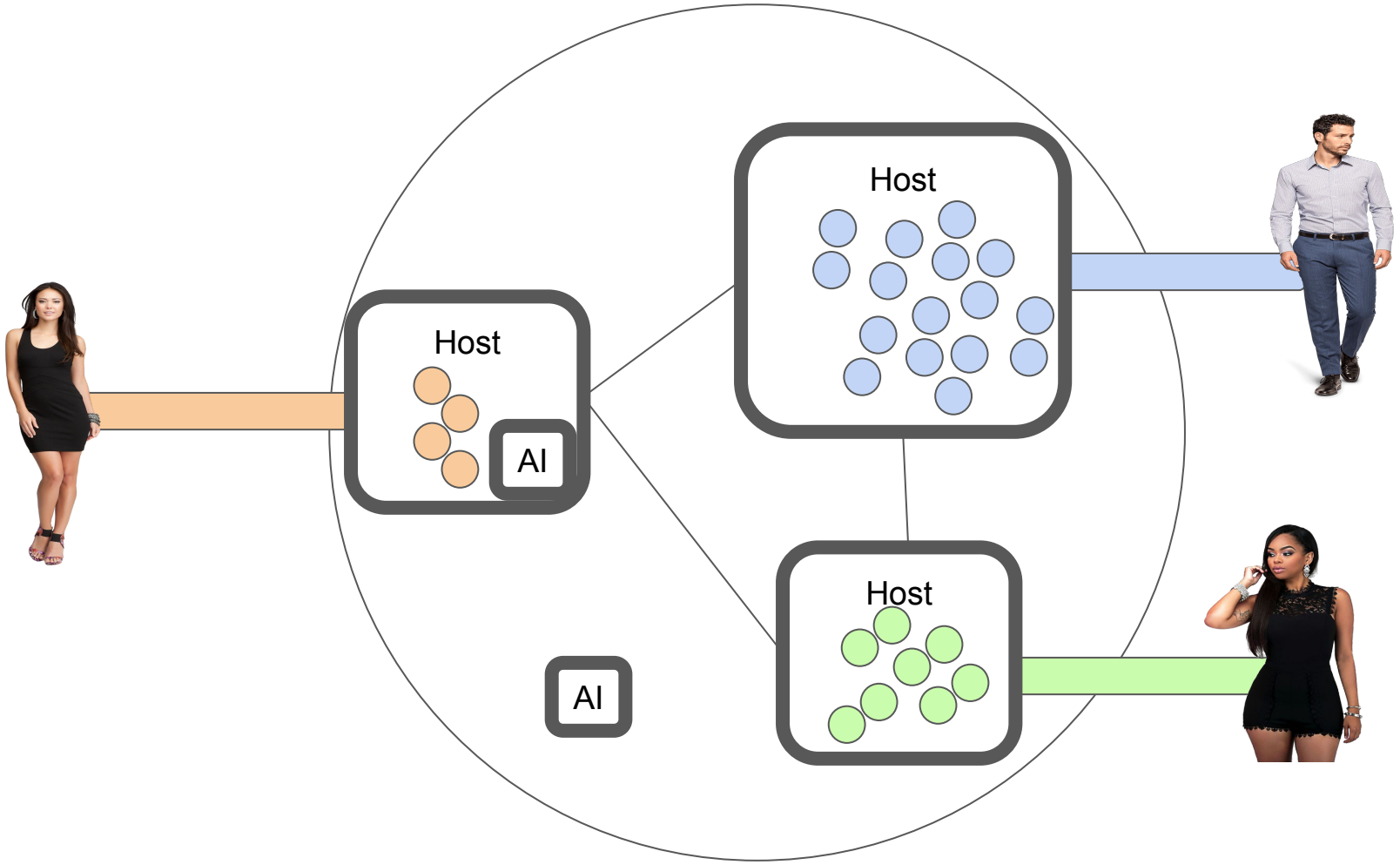
- Risks related to the data connections:
  - Type of protocol, TLS, MQTT, SFTP, etc,
  - Application Programmable Interface (API),
  - Broken authentication,
  - improper authorization validation

- Risks related to the data sharing:
  - Open share / Open discovery,
  - Request forgery,
  - Misconfiguration

- Risks related to the development of digital twin:
  - Insecure development life cycle,
  - Insecure code reuse

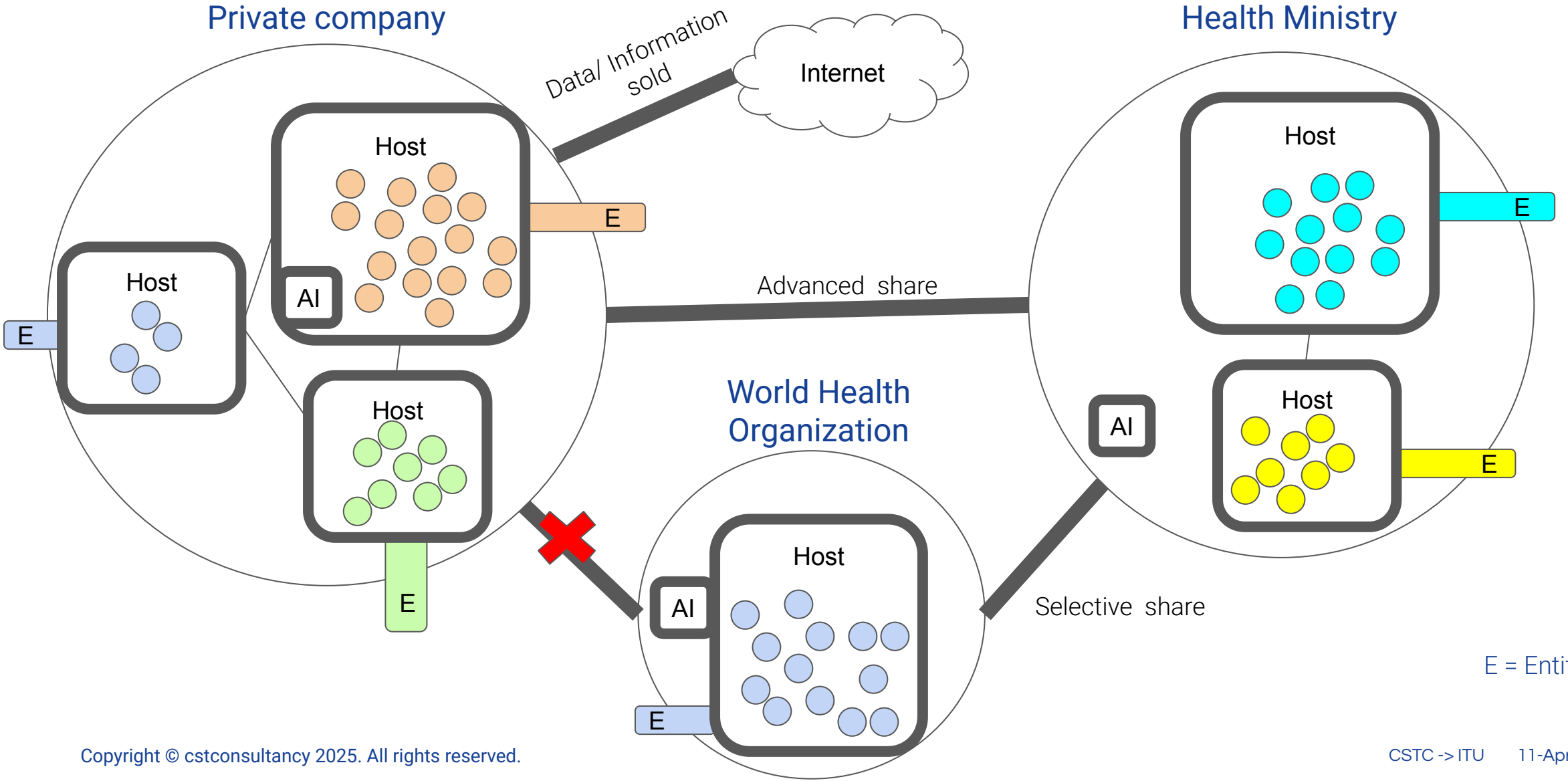
- Risks related to information security management:
  - Organizational risks,
  - People risks,
  - Technology risks

Digital Twin world/space and Artificial intelligence



What additional risks are involved?

Digital Twin Consortium and Backbone for Metaverse



How to contribute to the standard development

Identify which committee you might be interested in, eg:

ISO/IEC JTC1/SC 27 Information security, cybersecurity and privacy protection

ISO/IEC JTC1/SC 41 Internet of Things and digital Twin

ISO/IEC JTC 1/CG 2 Strategic coordination group on Metaverse

IEC SEG 15 Joint SEG with ISO - Metaverse

Liaise with your national committee
ISO https://www.iso.org/about/members
IEC https://iec.ch/national-committees

Thank you!

hello@cstconsultancy.com