Digital Twins

Digital twin technology, a prominent technology trend, creates virtual models of physical systems or processes, and it is expected to continue to grow in popularity in 2023. Digital twins are digital representations of physical objects, systems, or processes that can be used for simulation, analysis, and optimization. They are created by collecting data from sensors and other sources and using it to create a virtual model of the object or system being represented.

Digital Twin is at the forefront of the Industry 4.0 revolution facilitated through advanced data analytics and the Internet of Things (IoT) connectivity. IoT has increased the volume of data usable from manufacturing, healthcare, and smart city environments. The IoT's rich environment, coupled with data analytics, provides an essential resource for predictive maintenance and fault detection to name but two and also the future health of manufacturing processes and smart city developments , while also aiding anomaly detection in patient care, fault detection and traffic management in a smart city . The Digital Twin can tackle the chal- lenge of seamless integration between IoT and data analytics through the creation of a connected physical and virtual twin (Digital Twin). A Digital Twin environment allows for rapid analysis and real-time decisions made through accurate analytics.

A digital twin is a digital representation of a physical item or assembly using integrated simulations and service data. The digital representation holds information from multiple sources across the product life cycle. This information is continuously updated and is visualised in a variety of ways to predict current and future conditions, in both design and operational environments, to enhance decision making.

Digital Model

A digital model is described as a digital version of a pre- existing or planned physical object, to correctly define a dig- ital model there is to be no automatic data exchange between the physical model and digital model. Examples of a digital model could be but not limited to plans for buildings, product designs and development. The important defining feature is there is no form of automatic data exchange between the physical system and digital model. This means once the digital model is created a change made to the physical object has no impact on the digital model either way.

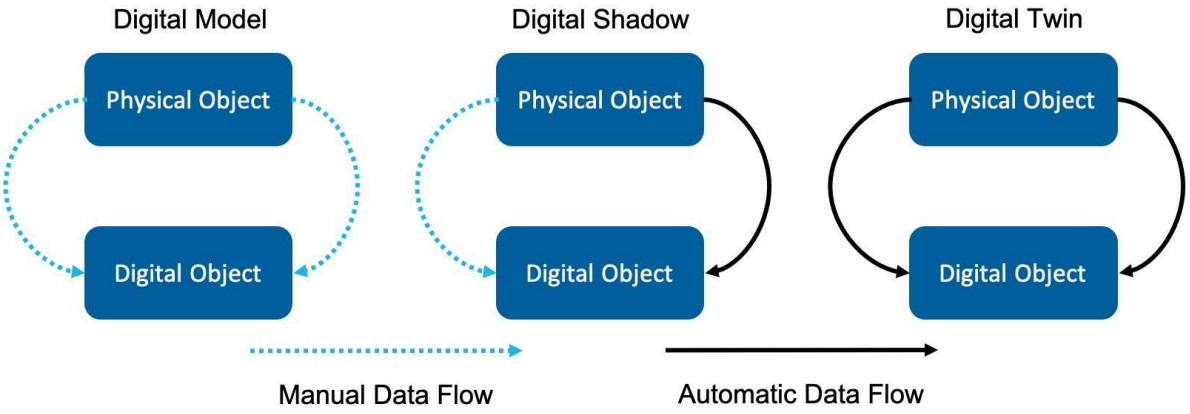
Digital Shadow

A digital shadow is a digital representation of an object that has a one-way flow between the physical and digital object. A change in the state of the physical object leads to a change in the digital object and not vice versus.

Digital Twin

If the data flows between an existing physical object and a digital object, and they are fully integrated in both directions, this constituted the reference "Digital Twin". A change made to the physical object automatically leads to a change in the digital object and vice versa. These three definitions help to identify the common mis- conceptions seen in the literature.

However, there are several misconceptions seen but they are not limited to just these specific examples. Amongst the misconceptions is the mis- conception Digital Twins have to be an exact 3D model of a physical thing. On the other hand, some individuals that think a Digital Twin is just a 3D model.



DIGITAL TWIN APPLICATIONS

The next part of this review focusses on the applications of Digital Twins. It will first start by looking at the potential ap- plications for Digital Twins, discussing the domain, sectors, and specific problems for Digital Twin technology. For the moment the term and concept of a Digital Twin are growing across academia, and the advancements in IoT and artificial intelligence (AI) are enabling this growth to increase, At this stage, the primary areas of interest are smart cities and manufacturing with some healthcare-related applications of Digital Twin technology found.

1) Smart cities

The use and the potential for Digital Twins to be dramatically effective within a smart city is increasing year on year due to rapid developments in connectivity through IoT.
With an increasing number of smart cities developed, the more connected communities are, with this comes more Digital Twins use. Not only this, the more data we gather from IoT sensors embedded into our core services within a city, but it will also pave the way for research aimed at the creation of advanced AI algorithms.

2) Manufacturing

The next identified application for Digital Twin is within a manufacturing setting. The biggest reason for this is that manufacturers are always looking for a way in which products can be tracked and monitored in an attempt to save time and money, a key driver and motivation for any man- ufacturer. Thus why Digital Twins look to be making the most significant impact within this setting. Likewise, with the development of a smart city, connectivity is one of the biggest drivers for manufacturing to utilise Digital Twins. The current growth is in line with the Industry 4.0 concept, coined the 4th industrial revolution, this harnesses the connectivity of devices to make the concept of Digital Twin a reality for manufacturing processes. The Digital Twin has the potential to give real-time sta- tus on machines performance as well as production line feedback.

It gives the manufacturer the ability to predict issues sooner. Digital Twin use increases connectivity and feedback between devices, in turn, improving reliability and performance. AI algorithms coupled Digital Twins have the potential for greater accuracy as the machine can hold large amounts of data, needed for performance and prediction analysis. The Digital Twin is creating an environment to test products as well as a system that acts on real-time data, within a manufacturing setting this has the potential to be a hugely valuable asset.

3) Healthcare

The healthcare sector is another area for the application of Digital Twin technology. The growth and developments enabling technology are having on healthcare is unprecedented as the once impossible is becoming possible. In terms of IoT the devices are cheaper and easier to implement, hence the rise in connectivity . The increased connectivity is only growing the potential application of Digital Twin use within the healthcare sector. One future application is a Digital Twin of a human, giving a real-time analysis of the body. A more realistic current application is a Digital Twin used for simulating the effects of certain drugs. Another application sees the use of a Digital Twin for planning and performing surgical procedures. Having the ability to simulate and act in real-time is even more paramount within healthcare as it can be the difference between life or death. The Digital Twin could also assist with predictive maintenance and ongoing repair of medical equipment. The Digital Twin within the medical environment has the potential along with AI to make life saving decisions based on real-time and historical data.

F/No. 034010769
INSP/RO S.K. Choudhary

Post-quantum cryptography: securing data in the age of quantum computers

Governments and organizations across the world are rushing to develop quantum computing platforms and advanced security algorithms to defend against such machines. One such example is the National Institute of Standards and Technology's Post-Quantum Cryptography Standardisation project. India has launched the National Quantum Mission. It will target developing intermediate scale quantum computers with 50-100 physical qubits in 5 years and 50-1000 physical qubits in 8 years. Just like bits (1 and 0) are the basic units by which computers process information, 'qubits' or 'quantum bits' are the units of process by quantum computers. The mission will help develop magnetometers with high sensitivity for precision timing (atomic clocks), communications, and navigation. It will also support design and synthesis of quantum materials such as superconductors, novel semiconductor structures and topological materials for fabrication of quantum devices.

The mission will also help developing:-

1. Satellite based secure quantum communications between ground stations over a range of 2000 km within India.
2. Long distance secure quantum communications with other countries
3. Inter-city quantum key distribution over 2000 km
4. Multi-node Quantum network with quantum memories

Four Thematic Hubs (T-Hubs) would be set up in top academic and National R&D institutes on the domains of Quantum Technology:

1. Quantum computation
2. Quantum communication
3. Quantum Sensing & Metrology
4. Quantum Materials & Devices

Security algorithm:

- Much of our current security is based on techniques such as RSA, elliptic curves, Diffie-Hellman key exchange and almost all of them rely on a few "hard" mathematical problems, such as factorisation and the discrete logarithm problem.
- In 1994, Peter Shor developed a quantum algorithm that can break all of these with ease.
- While Shor's technique poses a threat to certain security algorithms, there are alternative methods that remain unaffected.
- Lov Grover's quantum algorithm can often be fixed by increasing the key or password lengths.
- Some common "symmetric" security algorithms such as AES are not badly affected. (Symmetric key algorithms use the same password to lock and unlock the information.)

Post-quantum cryptography:

- Post-quantum cryptography involves exploring alternative techniques to counter vulnerabilities against quantum attacks.
- In cryptography, post-quantum cryptography (PQC) refers to cryptographic algorithms (usually public-key algorithms) that are thought to be secure against a cryptanalytic attack by a quantum computer.
- The problem with currently popular algorithms is that their security relies on one of three hard mathematical problems: the integer factorization problem, the discrete logarithm problem or the elliptic-curve discrete logarithm problem.
- All of these problems could be easily solved on a sufficiently powerful quantum computer running Shor's algorithm.
- While Shor's algorithm poses particular concerns for certain methods, the field has rapidly evolved with promising approaches such as lattice algebra, multivariate cryptography, isogeny-based techniques, and code-based cryptography.
- One promising technique, super singular isogeny Diffie-Hellman key exchange, was considered secure by many until it was utterly broken by Wouter Castryck and Thomas Decru last year.

Bits of physics:

We have developed circuits that can do logical computations incredibly fast and with astounding reliability. New kinds of gates can be built using the laser, maybe a prism "naturally" computes a square root or something. The principles of quantum mechanics enabled a set of gates that were utterly impossible to build using electronics. In other words, using quantum states to represent logic allows us to compute very differently. This new, different kind of computation is very powerful. Many things that were complex and cumbersome when run on electronic logic become incredibly simple on a quantum system.

Challenges:

This comes with its own problems. Current attempts are incredibly error-prone and have many missing pieces. However, many experts believe that this is inevitable and we will eventually develop such machines.

F/No. 107410436
SI/T Ravin Kumar

Edge Computing

Formerly a new technology trend to watch, cloud computing has become mainstream, with major players AWS (Amazon Web Services), Microsoft Azure and Google Cloud Platform dominating the market. The adoption of cloud computing is still growing, as more and more businesses migrate to a cloud solution. But it's no longer the emerging technology trend. Edge is.As the quantity of data organizations is dealing with continues to increase, they have realized the shortcomings of cloud computing in some situations. Edge computing is designed to help solve some of those problems as a way to bypass the latency caused by cloud computing and getting data to a data centre for processing. It can exist "on the edge," if you will, closer to where computing needs to happen. For this reason, edge computing can be used to process time-sensitive data in remote locations with limited or no connectivity to a centralized location. In those situations, edge computing can act like mini datacenters.

Amazon Web Services, Inc. (AWS):- is a subsidiary of Amazon that provides on-demand cloud computing platforms and APIs to individuals, companies, and governments, on a metered, pay-as-you-go basis. Clients will often use this in combination with auto scaling (a process that allows a client to use more computing in times of high application usage, and then scale down to reduce costs when there is less traffic). These cloud computing web services provide various services related to networking, compute, storage, middleware, IoT and other processing capacity, as well as software tools via AWS server farms. This frees clients from managing, scaling, and patching hardware and operating systems. One of the foundational services is Amazon Elastic Compute Cloud (EC2), which allows users to have at their disposal a virtual cluster of computers, with extremely high availability, which can be interacted with over the internet via REST APIs, a CLI or the AWS console. AWS's virtual computers emulate most of the attributes of a real computer, including hardware central processing units (CPUs) and graphics processing units (GPUs) for processing; local/RAM memory; hard-disk/SSD storage; a choice of operating systems; networking; and pre-loaded application software such as web servers, databases, and customer relationship management (CRM).

Microsoft Azure:- often referred to as is a cloud computing platform run by Microsoft. It offers access, management, and the development of applications and services through global data centers. It also provides a range of capabilities, including software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS). Microsoft Azure supports many programming languages, tools, and frameworks, including Microsoft-specific and third-party software and systems.Azure was first introduced at the Professional Developers Conference (PDC) in October 2008 under the codename "Project Red Dog." It was officially launched as Windows Azure in February 2010 and later renamed Microsoft Azure on March 25, 2014.

Google Cloud Platform (GCP):- offered by Google, is a suite of cloud computing services that provides a series of modular cloud services including computing, data storage, data analytics, and machine learning, alongside a set of management tools. It runs on the same infrastructure that Google uses internally for its end-user products, such as Google Search, Gmail, and Google Docs, according to Verma, Registration requires a credit card or bank account details.Google Cloud Platform provides infrastructure as a service, platform as a service, and serverless computing environments.

In April 2008, Google announced App Engine, a platform for developing and hosting web applications in Google-managed data centers, which was the first cloud computing service from the company. The service became generally available in November 2011. Since the announcement of App Engine, Google added multiple cloud services to the platform.

Google Cloud Platform is a part of Google Cloud, which includes the Google Cloud Platform public cloud infrastructure, as well as Google Workspace (G Suite), enterprise versions of Android and ChromeOS, and application programming interfaces (APIs) for machine learning and enterprise mapping services.

F/No. 041622299
HC/RO Vishwanath Swamy

Counter-Drone Techniques To Detect And Neutralise Hostile Drones

Though radar is a useful tool for detection of drones, there are limitations like low altitude, velocity of flying, and their small RCS, making it difficult to distinguish them from the noise and clutter present. Sometimes, multi-static radars are used to monitor, track, and analyse the energy back-scattered from rotating parts like propellers and rotors for drone.

Drone and anti-drone technologies will continue to evolve and co-exist. The next generation of unmanned aerial vehicles (UAVs) will be lighter, smaller, more complex, and be able to multi-task. Hence the necessity to figure out new, more effective ways of shooting these platforms down.

Hostile drones pose threat to military and strategic installations and public security. One way to engage an enemy with minimum casualties is using drones that do not carry human operators, use aerodynamic forces for lift, fly autonomously or are piloted remotely, are either expendable or recoverable, and can carry both lethal and non-lethal payloads.

Drones are becoming the preferred means for intelligence gathering, surveillance, reconnaissance, electronic warfare, strike missions, air combat, and search and rescue missions due to their capability to loiter, search, identify, and strike targets while minimising the collateral damage. Their civil applications include policing, firefighting, inspection of power lines and pipelines, delivering packages, etc.As drones are becoming increasingly versatile, stealthy, and convenient airborne weapons, there is need for hostile drones to be detected quickly, identified, localised, and neutralised. Counter-drone systems, also called counter-unmanned aerial systems (C-UAS), are used to detect and neutralise the hostile unmanned aerial systems while in flight to protect areas such as critical infrastructure, airports, large public spaces, and military installations.

RADAR

Radars are classified as 2D and 3D by the type of the phase array antenna used. 2D radars use passive electronically scanned array antennas (PESAs) and provide relatively large detection range. However, 3D radars use active electronically scanned array antennas (AESAs), have relatively short detection range, can se correct errors, and support wideband detection. 3D radars are preferred as they can estimate the altitude o target objects. Radar based detection systems offer longer range and constant observability compared wit RF scanners, but have regulatory limitations for use.

Acoustic sensors (microphones)

During flight the sound generated by the rotors can be utilised in detection, classification, and localisation of drones. Acoustic sensors, usually microphones or microphone arrays, are used to detect the sound generated and calculate the direction of the flight using algorithms such as multiple signal classification (MUSIC).Acoustic sensors can detect drones within the near-field and even those that are operating autonomously and not emitting RF radiations. they do not work very well in noisy environment, have very short range (max. 300-500m), and are mostly used along with other detection techniques.

Optical/infrared sensors

These sensors are essentially daylight or infrared (IR) scanners, which detect objects based on their appearance and motion features across consecutive frames. IR scanners are useful in conditions of low visibility.

Thermal detectors

The motors, batteries, and other on-board equipment of drones radiate significant amount of heat that imparts thermal signatures, which can be recognised by thermal sensors. Thermal detection has advantages in terms of weather resilience, identification availability, and lower costs, but the range is limited.

Hybrid detectors

Using a single method for detection may cause blind spots, making successful neutralisation difficult. Hybrid detection systems with sensor fusion technology and joint control system provide greater accuracy and installation flexibility.

Drone jamming

Drone jamming involves paralysing radio communication between the target drone and its controller to make it uncontrollable by using powerful interfering RF signals. The options include jamming the drone-controller link or jamming the GPS link so that it loses control of ‘auto-home’ facility.The jamming systems can be directional or omnidirectional. In directional jamming, the power is confined spatially, decreasing the possibility of

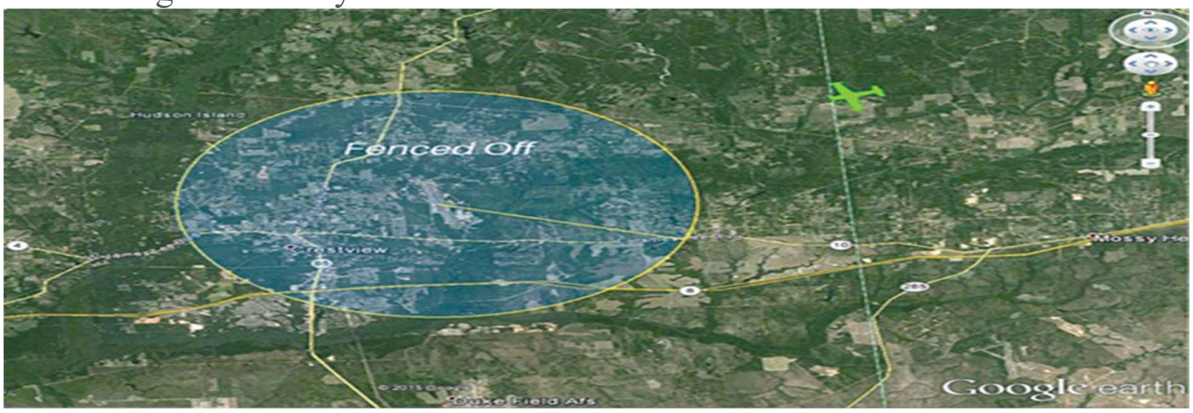
interference with the co-located RF devices/equipment. Stationary jammers are installed at a fixed location, whereas mobile jammers operate from portable devices that are handheld or vehicle-mounted.RF jammers are of medium cost and provide non-destructive neutralisation, have short range, may affect and/or jam other radio communications, and can result in unpredictable drone behaviour, such as unintentionally sending the drone to its target. They can cause significant unintended impacts, such as interference with the TV broadcasts, telecommunications, or even the air-traffic control systems.

GPS spoofers

Controllers use GPS satellites to navigate the drones. Fake GPS signals are used to spoof the communication with the satellites, preventing the drone from moving as intended by the controller. The drone is 'spoofed' into thinking it's somewhere else and loses control of auto-home facility and can be hijacked and diverted to a desired zone. Drone hijacking is an ideal approach, facilitating follow-up investigation.GPS spoofers are of medium cost, provide non-destructive neutralisation, have short range, and may affect and/or jam other radio communications in the area.

Geofencing

Geofence is a dynamically generated virtual perimeter for a real-world geographic area, which could be in a radius around a point location, or a predefined set of boundaries. In geofence neutralisation the target drones are prevented from approaching the pre-defined point or entering the defined boundaries, thus blocking them from trespassing.
Geofencing could be dynamic or static.



In dynamic geofencing the information regarding restricted area is continuously propagated. Static geofencing uses a flight permission information repository, which when accessed by the intruding drone denies it access beyond the intended point.Most commercial drones use internal auto-landing modules for safety. Geofencing is unable to disable these automatic landing systems.

Killer drones

Killer drones are employed to track and destroy the invading drones by physically striking them down. This technique requires reactive and real-time decision making, accurate target flying path estimation, and outstanding physical durability and mobility. Swarming killer drones with distributed intelligence and precise tracking systems are promising solution for drone fleet multi-faceted attacks.

High-power microwave pulses

High-power microwave (HPM) devices generate electromagnetic pulses (EMPs) capable of disrupting electronic devices. The EMPs interfere with the radio links and disrupt or even destroy the electronic circuitry by inducing damaging voltages and currents. As a result, the targeted drone falls uncontrolled instantly.

HPM devices use an antenna to focus the EMPs in the required direction damage. Within the range, EMPs provide effective non-destructive neutralisation, but have high cost, and create risk of unintentionally disrupting communications or destroying other electronic devices in the area.to reduce the potential collateral

High-energy lasers

High-energy lasers use high-powered extremely focused laser beams to destroy the structure and/or the electronics of the targeted drone. They are high-cost, carry risk of collateral damage and are bulky in size.

Nets and net guns

Firing a net at a targeted drone, or bringing a net into contact with it immobilises it by prohibiting the rotor blades from moving. Mainly, they are of three types:

1.Net cannons fired from the ground. These could be hand-held, shoulder-launched, or turret-mounted. They have limited effective range, anywhere from 20m to 300m, and can be used with or without a parachute for controlled descent of the captured drone.

2.Net cannons fired from another drone. These overcome the limited range of those fired from the ground and are normally used with a parachute for controlled descent of the captured drone.

3.Hanging net deployed from a 'net drone.' The targeted drone is captured by maneuvering a net-carrying drone towards it. The 'net drone' is normally capable of carrying the captured drone to a safe zone. However, if it is too heavy, the captured drone is released with a parachute for controlled descent, or it is allowed to crash. Physically capturing the drone facilitates a forensic examination and prosecution.

The ground-launched net cannons are semi-automatic with high accuracy and have a short range. The drone-deployed nets provide long range and low risk of collateral damage. Drone-deployed nets are imprecise and have long reload time.

Birds of prey

This technique takes advantage of the natural hunting instinct of the eagles, used by man for hunting for thousands of years. It is possible to train eagles to capture drones. This low-tech solution requires a lot of manpower and time for training and maintenance of these birds of prey (at least one year per bird).

Interception of the drone by these birds of prey can be quick and accurate with low risk of collateral damage. They are difficult to scale due to limited number of birds available and could be an air hazard at airports.

Integrated counter-drone systems

Integrated counter-drone systems are a match-and-mix of the technologies, depending on the specific use. In the integrated system the data from different sensors is collected, processed, and displayed in a user-friendly way. Software provides effective command, control, and communication (C3). The systems are mostly scalable, sensor-agnostic, and user-friendly. Some examples of the existing systems are:

Guardion Modular Counter–UAS System

It provides a protective shield against the threat of unauthorised drones to both civil and military installations.The system is used by the German Armed Forces and airports to provide countermeasures against threats, such as hostile/illegal intrusion, smuggling, and terrorist attacks. The features include early warning, automatic detection and classification, powerful core intelligence and C3, and flexible customized deployment capability.

DRDO-developed counter-drone system

A counter-drone system has been developed by the DRDO to enable the Indian Armed Forces swiftly detect, intercept, and destroy small drones using both the soft kill and hard kill options. Soft kill refers to jamming the hostile drone, while hard kill neutralizes the target drone.

The system uses radar that offers 360-degree coverage with detection of micro drones 4km away, electro-optical/infrared (EO/IR) sensors for detection of micro drones up to 2km, and a radio frequency (RF) detector to detect RF communication up to 3km. After detection it hands over the track for soft kill/hard kill.

The RF-jammer used for neutralisation is capable of jamming the signals of the hostile drone from a distance of 3km using the Global Navigation Satellite System (GNSS). The laser based hard kill system used can neutralise micro drones 150 metres to one kilometre away. The system is integrated through a command post.

Anti-drone innovative systems

Some innovative, low-cost and simple to use solutions are available for disabling the drones. SMASH 2000, an optical sight used in small arms for precision aiming, has been modified. The advanced version, SMASH 2000 Plus, uses built-in algorithms to provide capability to track and hit even very small drones flying at high speed at range up to 120 meters, both during day and nighttime.

DroneKiller is another standalone handheld anti-drone device available from IXI EW. The device using software-defined radio technology, operating on seven frequency bands, can neutralise drones up to a range of 1000 metres and be in active mode for up to two hours (eight hours in standby), weighs 3.4kg and is comfortable to carry.

F/No. 041699428
ASI/.T C VIJAY KUMAR

Acknowledgement

We are highly thankful for reading out this compilation and hope it will be useful for you in day to day professional and personal life. We would like to hear your interest areas, suggestions from you to make this newsletter more informative and interesting. Your views will definitely help us to create this newsletter as an effective medium to reach you with latest development in the fields of communication and technology.

R&D Team
CTC T&IT CRPF, Ranchi, Jharkhand
ctcit@crpf.gov.in