Assurance of Digital Twins for Safety-Critical Systems



Digital Twins are seen as a formative technology for the Internet of Things (IoT), central to future systems development. When Safety-Critical Systems fall in scope of Digital Twins, and it is clear they will, then proportionate assurance will be necessary. From work in support of his MSc thesis, Kevin King presents Principles to support the assurance of Digital Twins in their role in through-life safety assurance.

The Problem of Static System Assurance

Historically, when a product or system enters into service, the manufacturer presents an argument that their system is acceptably safe for its intended purpose when measured against its design intent, generally known as a system safety case, or in some fields, a safety assurance case. However, the arguments it sets out are typically static at the point of delivery, only evolving to reflect the system in service when a baseline update occurs, which is typically slow and reactive. There are many examples where system safety-cases have not kept track with their design intent, notably the Nuclear accidents at Three-Mile Island and Chernobyl, the Chemical accident at Bhopal and the Space Shuttle Challenger disaster. In all these cases, changes to the design, operating procedures or environmental envelope were contributory factors to the accident.

Moving to a Dynamic Assurance Solution

These examples were back in the 20th century and in recent years systems have become significantly more complex, predominantly borne out of a comparable increase in the resources available to support design, implementation and operational service. Parallel to this complexity growth has been the evolution of smart technologies to enable resource management of these ever more complex systems in a world where consumers expect 'more for less'. Crucially, these proposed smart solutions consider the systems they underpin through their entire lifecycle; pointing to the need for a more dynamic approach to their assurance, an approach that may have mitigated the incidents mentioned and many others.

For some time, industry has been seeking to understand what this complex future really means; with a broadly held view that it will be based on the 21st century concept of the IoT. Consequently, systems are expected to become more dynamic, a step change from the static solutions of the past. The expansion of system complexity, real-time data explosion, and growth in novel technologies such as Cloud Computing, Big Data Analytics, Machine Learning and Artificial Intelligence will all play their part in these dynamic IoT-based systems.

One technology proposed to underpin this new, dynamic world is the Digital Twin. A term first advocated by Grieves and Vickers in 2002 [1] and seen as a catch-all for the burgeoning collection of 'smart' technology-based assets that could be seen to collectively mirror a physical system. Crucially, the Digital Twin is seen as remaining interconnected with what could be viewed as its 'Physical Twin', through its entire life.

From that earliest formulation, there has been a growing view, notably since 2017, that promotes Digital Twins as the answer to the complexity/resource conundrum presented by the IoT. Equally, the dynamic nature of the Digital Twin is seen by some as a means to maintain system safety through life, albeit theoretically.

Issues of Confidence with Digital Twins

Considering the complexity of a Safety-Critical System, the Digital Twin paradigm adds a further dimension, which the author believes raises fundamental questions around maintaining confidence that it will provide an acceptable level of assurance of the safety of its Physical Twin dynamically through its in-service life.

Digital Twins have for some time been seen by some as an immature construct, with Gartner positioning them at the 'peak of inflated expectation' in the August 2018 issue of their Hype Cycle with the 'Digital Twin of the Person' still climbing the innovation trigger in 2020. To gain confidence as the concept matures, if Digital Twins are to become a mainstream, productive technology, then it is appropriate to consider what issues might hamper their development.

There are lots of positives to support Digital Twins in a potential safety-assurance role in service, however, there are some significant issues to ponder, notably:

- **Environmental Similitude:** Can we be certain the virtual environment of the Digital Twin equates absolutely to the substantive environment of its Physical Twin?
- **Twin Divergence:** Can we be certain that the twins will maintain their sibling bond? Will one or other of them diverge?
- **Twin Utility:** A view that a Digital Twin emulating 100 percent of its Physical Twin is unrealistic. A Digital Twin will only be of true value if it associates data from the Physical

Twin with processes in the digital model seen as useful, in context of the physical systems operation.

- **Data Practicalities:** Vast amounts of data are predicted to be available to the Digital Twin. How that data is collected, filtered, analysed and put to use is seen as essential for the Digital Twin to be of value, with some researchers proposing the use of Big Data Analysis to address traditional frailties. Equally, concerns exist over protocol mismatches across the data interconnection.
- **Data Ownership:** Digital Twins' life-blood is the data it receives from its Physical Twin, but who owns that data? If fed from the operator of the physical system, how content will they be for their data to be fed back to the entity maintaining the Digital Twin? Is there scope for an operator to give their data not only to the manufacturer of a device but also a competitor, contracted to manage the Digital Twin?
- **Ethical and Societal Impact:** What if the data fed to or derived by the Digital Twin is in any way sensitive? This is of utmost relevance in the health care sector where concerns over data privacy, derived benefits and transparency of use are key. Will Digital Twins provide therapeutic solutions or advise on 'enhancements' and who will be able to afford their personal medical replicant?
- **Managing the Twins:** The point in the lifecycle of the physical system at which its Digital Twin is born is crucial to their ongoing relationship, as is how it endures through the physical system's life. Tools exist to evaluate the performance of physical systems; equivalents need to be considered to manage the Digital Twin to maintain the digital to physical bond.
- **Hyperbole:** Some researchers believe that by 2021 around half of large companies will be using Digital Twins. This links back to the hype mentioned earlier but the author believes is unrealistic.
- **Cost Effectiveness:** Creating Digital Twins for one-off complex, Safety-Critical Systems is seen as time consuming and costly when weighed against the benefits the Digital Twin provides. Significant upfront costs of Digital Twin development may not be viewed across the whole life of the physical system, especially in a keenly contested consumer world where 'cost to market' is an essential factor.
- **Incongruent Digital Twins:** Although generally seen as whole lifecycle assets, there is a view that in some sectors, Digital Twins will be developed focussing solely on characteristics of the design and build phase of a system. Once that system enters into service a fresh 'in-service' Digital Twin will be developed, potentially by a different organisation (service provider) or even a collection of them. There is scope therefore for the 'in-service' Digital Twin to be distinct from its design and build predecessor.

Many researchers are focussing on case studies where Digital Twins can be applied, in effect presuming the concept of Digital Twins is established and not considering sufficiently the key facets of the Digital Twin and notably, where targeted at Safety-Critical Systems, the role the Digital Twin may play in the assurance of the safety-related aspects of that physical system.

Key Attributes of a Digital Twin

Before proceeding to set out an approach to support the assurance of Digital Twins, it is appropriate to understand exactly what a Digital Twin is. Many definitions exist; breaking these down and considering across research in this area, Digital Twins are seen to have the following key attributes:

- The precise, ultra-high-fidelity replication of relevant facets of a physical system including the processes, people, interfaces and environment with which it interacts
- A unique portrayal of an instance of a physical system in a close one-to-one relationship
- The effective use of real-world data to iteratively maintain the sibling bond between the digital and physical twins through the whole product lifecycle
- A data interconnection that provides consistency and context between the digital and physical twins
- The ability to effectively simulate and predict events without impacting the physical twin
- The ability for the physical twin's performance to be enhanced, life to be extended and operating costs reduced through learning from its Digital Twin
- Components that exist wholly in the virtual world and can potentially be widely distributed
- Ability to provide quantifiable reliability and digital certification of the physical twin

Distilling these attributes, the author has formed a pertinent definition of a Digital Twin.

Digital Twin
A dynamic, comprehensive, wholly digital one-to-one representation of a physical system, encompassing its structure, components, properties, users, behaviours, interfaces, and target environments. The Digital Twin shall be born when the embryo of its physical sibling is conceived and should evolve dynamically, remaining intrinsically linked to it. The sibling bond shall be maintained through the life of the physical system through a data interconnection, providing real-world, near real-time data. The Digital Twin shall be able to effectively simulate and predict events without impacting the physical system, enabling enhanced performance, supporting potential life extension, and reducing operating costs.

When is the Digital Twin of most benefit?

If assurance on entry into service is a mature concept across industry, why do we still witness industrial incidents such as Deepwater Horizon? It would seem that systems assurance wanes over time. Theoretical research sees the Digital Twin as a core technology in systems management through life, but can we be certain once their Physical Twin enters into service that will include an ongoing assurance role? The critical issue is the symbiosis between the Digital and Physical Twins which is expected to endure through the systems life. The evolving life of systems in service would appear to be a fundamental factor influencing the role of Digital Twins. Thus, it makes sense to understand the best solutions to both assure Digital Twins and provide sufficient confidence in their role in assuring their Physical Twin.

Research and industry have focussed across a range of areas where Digital Twins are seen as beneficial, many of these being safety-critical, including autonomous vehicles [3], healthcare [4], aerospace [5], and the Rail Sector [6].

Of particular interest to the author is the defence industry which finds its systems no longer immune to the IoT explosion. The United Kingdom's Defence Science and Technology Laboratory (DSTL) have defined the Internet of Military Things (IoMT), which is expected to employ the technologies and concepts of the IoT. Although defence systems historically have run in isolation for reasons of safety and security, the evolution of web-based Maintenance Management Systems coupled with budgetary efficiencies brings defence systems into the scope of the Digital Twin. Linked to the Internet of Military Things, it would also seem realistic to expect a data explosion in defence systems employing secure cloud-based data management e.g. to interlink battlefield assets with command posts, a 21st century implementation of the datalink technology of the 1990s. Digital Twins are likely to play as important a role in the IoMT as they are in the IoT, making their capability for providing 'sentient-assurance' through the life of a system as important in that arena.

Sentient Assurance

It would seem logical that systems assurance will need to keep pace with the 'smart', dynamic solutions within the new IoT-based world and evolve beyond the fundamental shortcomings of the static, reactive approach to a more dynamic, proactive, 'sentient-assurance' methodology. As a 'living' concept, Digital Twins could play an intrinsic role in providing that 'sentient-assurance'; ensuring the Physical Twin they support maintains its design intent through its operational life. Where the system being twinned is safety-critical, there is an added requirement to consider if any certification or accreditation of the Digital Twin is required.

Digital Twins are gaining traction as a 'sentient-assurance' methodology but dependence on them could come at a cost. If they are relied upon without any plausible certification or accreditation, it is conceivable that they could provide a misleading view of confidence in the safety of their Physical Twin. It would appear essential that a credible methodology is needed against which Digital Twins can be established to provide the 'sentient-assurance' of Safety-Critical Systems through their entire lifecycle, notably when in service. This methodology would also support the certification and accreditation being sought.

The Digital Twin Assurance Gap

Commonly, approaches to assurance of Safety-Critical Systems need to confidently demonstrate that all risks to life from the system have been considered with all intolerable risks eliminated and all other risks, through mitigation, reduced As Low As Reasonably Practicable (ALARP) in line with relevant guidelines, e.g. The Office of Rail Regulation, Railway Safety Principles and Guidance [7]. In many domains that approach is further underpinned by some form of independent accreditation or certification, such as the Certificate of Airworthiness sought by Farnell et al. [8]. For Digital Twins to be seen as a key pillar in the assurance of Safety-Critical Systems then it is sensible to believe they will require equivalent objective endorsement, likely accreditation and certification.

Glaessgen and Stargel [9] believe Digital Twins will "revolutionise certification". However, the author's research across the fields of safety governance, accreditation, and certification was unable to find examples of Digital Twin certification that address the need identified. There is an assurance gap that needs to be addressed. That research covered the main sectors where Safety-Critical Systems predominate, and the related standards, e.g. SAE ARP 4761, ISO 14971, ISO 26262, Def Stan 00-056, ISO 61508.

As the NZ Government's Chief Digital Officer states [10] "A principles-based approach provides confidence in the delivery of outcomes without resulting in excessive levels of assurance". Therefore, to support the assurance 'gap' some generic principles would seem appropriate.

Several researchers have proposed what they term frameworks or models applicable to Digital Twins, some in a system safety context and some in related technologies such as Cyber Physical Systems. Importantly, none explicitly address the endorsement of Digital Twins for Safety-Critical Systems. Rather than dismiss these various works for not providing the whole solution to the gap, it seemed sensible to consider the benefits they present that could be valuable in considering assurance in the Digital Twin paradigm.

The Approach to Developing Digital Twin Assurance Principles

Rather than defining a framework or model, it was assessed that supporting principles would provide a more generic, pan-sector solution for the assurance gap. In developing these principles, it was necessary to understand what form they would take and what methodology should be applied to ensure the results were credible and repeatable.

There are two main styles of principles; they are either based on characteristics and behaviours as with the Gemini Principles [13], where artefacts exhibiting a sufficiency of the characteristics and behaviours can be considered compliant with the principles, or rule-based, as in the Software Safety Principles [14] where compliance with the rules means an artefact has met the principles. This research employed the former style given the rapidly changing theories in the Digital Twin paradigm and need to understand the characteristics exhibited by Digital Twins that fall in scope of assurance.

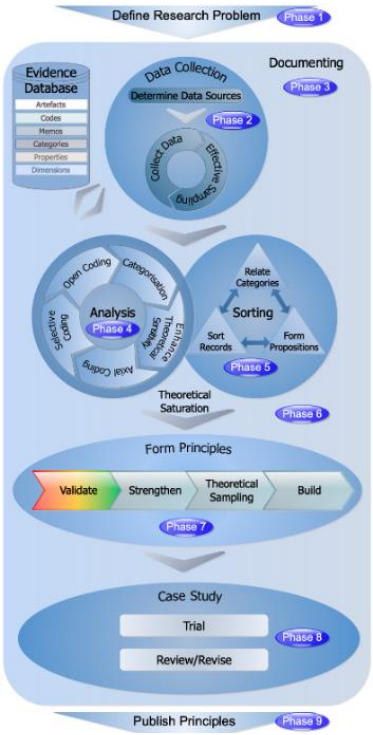


Figure 1 Refined Grounded Theory

The methodology chosen to support the development of assurance principles needed to be set out clearly to maintain credibility as the Digital Twin paradigm moves towards the 'Plateau of Productivity' [2]. Considering the scope of material available across industry and academia and the wide range of theories they present made it difficult to approach data analysis with any preconceptions. Practically, the approach chosen needed to reduce instability in the results by ensuring the design is repeatable within agreed parameters. Significant variability of outcomes from the methodology would cast doubt over its

veracity. Three aspects needed to be ensured. Firstly, the chosen technique needed to stand up to academic scrutiny. Secondly, the methodology needs to be sufficiently generic to hold value across all sectors of industry. Finally, the themes that are derived by the application of the methodology must be grounded in real-world data to be seen as useful. This directed to the use of a refined application of the social sciences-based technique of Grounded Theory Analysis (GTA) (Figure 1). As with all qualitative approaches, themes emerge from the analysis undertaken. Importantly by employing GTA, those themes are 'grounded' uniquely in the chosen datasets analysed. Furthermore, GTA is structured around a set of clearly defined activities, offering consistency, credibility and repeatability for the analysis undertaken.

Details of the refinement of the GTA and how it was applied are in the author's paper on Digital Twin Assurance presented at SSS '21 [12].

The Principles

Application of the refined GTA led to the emergence of 7 principles as set out below. Should a Digital Twin of a Safety-Critical System exhibit these principles then it could be considered to be providing an acceptable level of assurance of its Physical Twin.

Detailed objectives have also been proposed for each principle, but for brevity, these are not included in this article. Rather they can be found in the author's paper on Digital Twin Assurance presented at the Safety-Critical Systems Symposium 2021 [12].

In addition to the emergent principles, it is appropriate to consider the level of risk the Digital Twin presents to its Safety-Critical Physical Twin. Therefore, an additional +1 principle is proposed in line with the approach taken by Hawkins et al in defining the Software Safety Principles [14].

1 Conformance



Outline

All constituent elements of a Digital Twin must conform to the context and intended use of the Physical System with which it is being twinned. They must also conform to any applicable Digital Twin standards and regulations in place. Importantly such conformance must be maintained through the life of the Physical System which itself would be expected to conform to relevant standards for the sector in which it is operating.

Digital Twins will be expected to align to a specified level of data abstraction consistent with the equivalent levels in their Physical Twin.

Rationale

For a Digital Twin to be of any value it needs to be appropriately aligned to the Physical System it is to be twined with centred around its intended purpose. The extent of that veracity depends on:

1. The quality of the data that the twin will be reliant on
2. The fidelity of the algorithms within the twin's constituent models
3. The conformity of the source code within the digital representation
4. The quality of the twin's output
5. The level of safety criticality in the Physical Twin.

2 Awareness



Outline

Digital Twin processes of Safety-Critical Systems will need to be able to be prognostic/proactive and identify future unsafe events through perception of the Physical Twin's environment, comprehension of the current situation, and projection of future states. Such situational awareness and decision making should trigger mitigating controls in the Safety-Critical Physical Twin which positively influence the path it takes. Digital Twin awareness should also mitigate against divergence across instances.

Rationale

Consideration needs to be taken of the predictive nature of assurance that technologies such as Machine Learning and Artificial Intelligence require. For Digital Twins to be perceptive (i.e. have situational awareness and make appropriate decisions to ensure the Physical Twin remains acceptably safe), the whole asset lifecycle is an essential element of this paradigm.

3 Interoperability



Outline

Digital Twins of Safety-Critical Systems must be able to establish equivalence between their constituent representation models, the 2-way data interconnection and their Physical Twin. Open standardised data formats and sector independence must form the basis to enable such interoperability.

Rationale

Without a clear understanding of data formats, standards and hosting domains there is scope for Digital Twins to grow incongruent with their Physical Twin. Equally, for safety-critical applications it is essential that the Digital Twin is able to account for changes in standards and data formats through the service life of its Physical Twin.

4 Credibility



Outline

For Digital Twins to be credible, the relationship between them and their Physical Twin needs to be relevant, assured, secure and maintained at an appropriate level of integrity. All models that constitute the Digital Twin and all data that it interacts with need to consistently be of an acceptable quality. Evidence of the Digital Twin's credibility needs to be maintained in accordance with the *Curation* principle.

Rationale

Digital Twins need to maintain a level of similitude with their Physical Twin conforming to their design intent (which may have evolved), otherwise the assurance they provide cannot be considered credible.

The information interchange between Digital and Physical Twins is critical, the life-blood of their relationship. The integrity of that information is therefore essential.

5 Curation



Outline

For Digital Twins to provide precision in supporting the assurance of their Physical Twin, it makes sense that all artefacts within the Digital Twin paradigm are maintained in a configured, orderly way with assured records. Curation in this way provides an audit trail of changes to the Digital Twin to support the *Conformance* and *Evolution* principles.

Rationale

In Safety-Critical applications, to ensure a Digital Twin maintains conformance with its requirements, design and through-life operation, it is essential that consistency of performance is maintained. Notably, given the impact of Machine Learning and Artificial Intelligence this should include all artefacts in the Physical Twin and Data Interconnection.

6 Evolution



Outline

Digital Twins are expected to grow in parallel to the growth in their Physical Twin. For Safety-Critical Physical Twins that growth needs to be in a controlled manner facilitated by assured protocols and facets of the *curation* principle.

Rationale

Cyber Physical Systems that Digital Twins will be related to will evolve through their service life. They will likely involve Artificial Intelligence and Machine Learning technologies and be repurposed during their working life. The Digital Twin will need to evolve to maintain that relationship.

7 Clarity



Outline

For Digital Twins of Safety-Critical Systems it is appropriate to have clarity around the safety-related goals and priorities of their Physical Twin and the expectations of the owners/operators of it. This clarity needs to permeate through all artefacts in the virtual world of the Digital Twin.

Rationale

Aligned to the *Evolution* principle, it is sensible to develop a clear understanding of the functionality of all artefacts of the Digital Twin from cradle to grave of its Physical Twin. Clarity would also provide benefit in the structure and management of relationships throughout the Digital Twin Paradigm. Not just the inter-relationships betwixt Digital and Physical Twins but also the intra-relationships between the virtual components (models) in the Digital Twin.

+1 *Proportionality*



Outline

Across all 7 principles it is important that the effort applied is balanced against the level of risk the Digital Twin presents in the assurance of the safety properties of the Safety-Critical System it is supporting.

Rationale

In the context of Safety-Critical Systems, excessive effort expenditure to assure Digital Twins of low-risk Physical Systems is considered disproportionate to the management of that risk in line with the principles set out in the UK Health and Safety Executive Process "Reducing risks, protecting people". The application of these principles for Digital Twin Assurance is seen as requiring a similar approach to proportionality of application.

NOTE: This principle will need to adapt to account for changes in the required level of assurance where the Digital Twin is related to Machine Learning/Artificial Intelligence based Physical Systems.

Related Work

During this research, it has become evident that an ISO standard for Digital Twins (BS EN ISO 23247-1) is under development. Currently, that draft standard does not consider safety-assurance.

It is envisaged that parallel activities discussing issues of cyber-security in Digital Twins will ensue, so why not overlay this research onto that subject? The author is aware there are security into safety principles in the form of a new IET code of practice [16] and plans to engage in that arena to build on the Code of Practice.

The majority view appears to be that Digital Twins will by their nature be built on software. This raises a question over levels of Digital Twin integrity and whether BS EN 61508 and Safety Integrity Levels (SIL) need to be considered in the context of Digital Twins. Also, worth considering are Levels of Digital Twin Assurance supporting levels of data abstraction and safety criticality, akin to the Data Safety Assurance Levels [15].

Conclusion

This research has presented a set of 7+1 pan-sector assurance principles to provide confidence in the capability of a Digital Twin to safely support a Safety-Critical System.

Accepting that in reality the Digital Twin phenomenon is still in its infancy, if we are not careful, industries will run head-long into implementing them and trip over some substantial assurance hurdles they don't understand, and crucially, are not being required to by their independent regulator or relevant standards. Importantly, the timeframe to Digital Twin maturity is also uncertain.

There is a clear need for these principles, however, that must be caveated in scope of the 'hyped' domain of Digital Twins from which they evolved. Equally, it would be illogical to promote them as any form of panacea to the assurance need without a sufficiency of empirical evidence to support such promotion. This aligns with the view of Rae et al. [17] who believe that "safety science" needs to be firmly bedded in reality.

It seems sensible that, aligning with their manifesto, future practical work is enacted across industry to strengthen the foundations of the 7+1 principles before they can be considered substantively plausible and importantly are allowed to extend or evolve. It is naïve to expect the researcher to move the principles into that plausible space in isolation; the principles need exposure.

References

[1] M. Grieves and J. Vickers, 'Digital Twin: Mitigating Unpredictable, Undesirable Emergent Behavior in Complex Systems', In: Transdisciplinary Perspectives on Complex Systems 2017, pp. 85-113.

[2] K. Panetta, '5 Trends Drive the Gartner Hype Cycle for Emerging Technologies, 2020', Gartner, 18 August 2020 [Online]. Available: https://www.gartner.com/smarterwithgartner/5-trends-drive-the-gartner-hype-cycle-for-emerging-technologies-2020 [Accessed: 20-Oct-2020].

[3] M. Sharma and J. P. George, 'Digital Twin in the Automotive Industry: Driving Physical-Digital Convergence', White Paper, TATA Consultancy Services, 2018.

[4] K. Bruynseels, F. Santoni de Sio and J. van den Hoven, 'Digital Twins in Health Care: Ethical Implications of an Emerging Engineering Paradigm', Frontiers in Genetics, vol. 9, 13 Feb 2018.

[5] H. Aydemir, Z. Ugur and D. Umut, 'The Digital Twin Paradigm for Aircraft Review and Outlook,' 2020, doi: 10.2514/6.2020-0553.

[6] R. Tomar, J. Piesk, H. Sprengel, E. Isleyen, S. Duzgun and J. Rostami, 'Digital twin of tunnel construction for safety and efficiency', Proceedings of the World Tunnel Conference 2019 pp. 3224-3234, 2019.

[7] Office of Rail Regulation, Railway Safety Principles and Guidance, UK Health and Safety Executive, 2005.

[8] G. P. Farnell, A. J. Saddington and L. J. Lacey, 'A new systems engineering structured assurance methodology for complex systems', Reliability Engineering & System Safety, vol. 183, pp. 298 - 310, 24 Nov 2018.

[9] E. H. Glaessgen and D. S. Stargel, 'The Digital Twin Paradigm for Future NASA and U.S. Air Force Vehicles', 53rd AIAA/ASME/ASCE/AHS/ASC Structures, Structural Dynamics and Materials Conference, vol. 9, 14 Jun 2012.

[10] NZ Government's Chief Digital Officer, 'Principles of good assurance', 2019 [Online]. Available: https://www.digital.govt.nz/standards-and-guidance/governance/system-assurance/all-of-government-portfolio-programme-and-project-assurance-framework/principles-of-good-assurance [Accessed: 20 Oct 2020]

[11] V. Bolbot, G. Theotokatos, L. M. Bujorianu, E. Boulougouris and D. Vassalos, 'Vulnerabilities and safety assurance methods in Cyber-Physical Systems: A comprehensive review', Reliability

Engineering & System Safety, vol. 182, pp. 179 - 193, 2019.
[12] K.C. King, 'Digital Twins for Safety-Critical Systems: A rational approach to forming principles to support their role in safety assurance', Feb 2021, Proceedings of the 29th Safety-Critical Systems Symposium, UK.
[13] Bolton A, Enzer M, Schooling J et al, 'The Gemini Principles: Principles to guide the development of the National Digital Twin,' ed. Centre for Digitally Built Britain: Centre for Digitally Built Britain, 2018.
[14] R. D. Hawkins, I. Habli and T. P. Kelly, 'The Principles of Software Safety Assurance', presented at the International System Safety Conference, Boston, USA, 01-Aug-2013.
[15] Data Safety Initiative Working Group (DSIWG), Data Safety Guidance, v3.3. SCSC-127F (https://scsc.uk/scsc-127F), SCSC, 2021.
[16] Williams, P. and St. John Green, M. 'IET Code of Practice for Cyber Security and Safety', The Institute of Engineering and Technology, v1.0 ISBN 978-1-83953-318-1, 2020.
[17] A. Rae, D. Provan, H. Aboelssaad, and R. Alexander, "A manifesto for Reality-based Safety Science," Safety science, vol. 126, 02/12 2020, doi: 10.1016/j.ssci.2020.104654.

Kevin King

Kevin is Product Safety Functional Manager for BAE Systems Maritime Services, based in Portsmouth. He has over 35 years' experience in the defence industry initially as a software engineer, but for the last 12 years working in Product Safety across a wide portfolio of products including torpedoes, radars, small boats and training systems. Kevin has recently completed an MSc in Safety-Critical Systems Engineering at the University of York. His thesis for that degree forming the basis for this article.

All opinions expressed in this article are entirely his own and do not reflect the views of his employer.

this article is © BAE Systems PLC.
All images are copyright the author unless stated below:
Digital Twin Header image: ID 128043723 © Leowolfert | Dreamstime.com
Icons: free resource from www.flaticon.com [Accessed 2nd July 2020].

SCSC
FOR EVERYONE WORKING IN SYSTEM SAFETY

Seminar: Safety Culture Developments

THE SAFETY-CRITICAL SYSTEMS CLUB, Seminar:

Safety Culture Developments

Tuesday 13 April, 2021 - Zoom

This online seminar, held from 14:00-16:30 UK time, will look at new developments in Safety Culture and will feature results from the SCSC SCWG Online Survey. Further details TBA.