

Draft NISTIR 8356

# Considerations for Digital Twin Technology and Emerging Standards

Jeffrey Voas  
Peter Mell  
Vartan Piroumian

This publication is available free of charge from:  
<https://doi.org/10.6028/NIST.IR.8356-draft>

Draft NISTIR 8356

# Considerations for Digital Twin Technology and Emerging Standards

Jeffrey Voas  
Peter Mell  
*Computer Security Division  
Information Technology Laboratory*

Vartan Piroumian  
*Independent Consultant*

This publication is available free of charge from:  
<https://doi.org/10.6028/NIST.IR.8356-draft>

April 2021



U.S. Department of Commerce  
*Gina M. Raimondo, Secretary*

National Institute of Standards and Technology  
*James K. Olthoff, Performing the Non-Exclusive Functions and Duties of the Under Secretary of Commerce  
for Standards and Technology & Director, National Institute of Standards and Technology*

50 National Institute of Standards and Technology Interagency or Internal Report 8356  
51 34 pages (April 2021)

52 This publication is available free of charge from:  
53 <https://doi.org/10.6028/NIST.IR.8356-draft>

54 Certain commercial entities, equipment, or materials may be identified in this document in order to describe an  
55 experimental procedure or concept adequately. Such identification is not intended to imply recommendation or  
56 endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best  
57 available for the purpose.

58 There may be references in this publication to other publications currently under development by NIST in accordance  
59 with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies,  
60 may be used by federal agencies even before the completion of such companion publications. Thus, until each  
61 publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For  
62 planning and transition purposes, federal agencies may wish to closely follow the development of these new  
63 publications by NIST.

64 Organizations are encouraged to review all draft publications during public comment periods and provide feedback to  
65 NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at  
66 <https://csrc.nist.gov/publications>.

67

68 **Public comment period: *April 16, 2021 through June 16, 2021***

69 National Institute of Standards and Technology  
70 Attn: Computer Security Division, Information Technology Laboratory  
71 100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930  
72 Email: [nistir-8356-comments@nist.gov](mailto:nistir-8356-comments@nist.gov)

73 All comments are subject to release under the Freedom of Information Act (FOIA).

74

75

## Reports on Computer Systems Technology

76 The Information Technology Laboratory (ITL) at the National Institute of Standards and  
77 Technology (NIST) promotes the U.S. economy and public welfare by providing technical  
78 leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test  
79 methods, reference data, proof of concept implementations, and technical analyses to advance the  
80 development and productive use of information technology. ITL's responsibilities include the  
81 development of management, administrative, technical, and physical standards and guidelines for  
82 the cost-effective security and privacy of other than national security-related information in federal  
83 information systems.

84

85

### Abstract

86 Digital twin technology enables the creation of electronic representations of real-world entities  
87 and the viewing of the state of those entities. Its full vision will require standards that have not  
88 yet been developed. It is relatively new although it uses many existing foundational technologies  
89 and, in many cases, appears similar to existing modeling and simulation capabilities. This report  
90 attempts to provide clarity in understanding the concept and purpose of digital twins. It offers a  
91 new definition for a digital twin, and describes characteristics, features, functions, and expected  
92 operational uses. The report then discusses novel cybersecurity challenges presented by digital  
93 twin architectures. Lastly, it discusses traditional cybersecurity challenges as well as trust  
94 considerations in the context of existing NIST guidance and documents.

95

96

### Keywords

97 computer cybersecurity; control; digital twins; instrumentation; real-time command; real-time  
98 monitoring; simulation; standards; testing; trust; use case scenarios.

99

100

## Audience

101 This publication is accessible for anyone desiring to understand the envisioned capabilities of  
102 digital twin technology as well as the associated cybersecurity and trust issues. It is particularly  
103 applicable to developers of digital twin standards as well as implementers of the technology.

104

105

## Call for Patent Claims

106 This public review includes a call for information on essential patent claims (claims whose use  
107 would be required for compliance with the guidance or requirements in this Information  
108 Technology Laboratory (ITL) draft publication). Such guidance and/or requirements may be  
109 directly stated in this ITL Publication or by reference to another publication. This call also  
110 includes disclosure, where known, of the existence of pending U.S. or foreign patent applications  
111 relating to this ITL draft publication and of any relevant unexpired U.S. or foreign patents.  
112

112

113 ITL may require from the patent holder, or a party authorized to make assurances on its behalf,  
114 in written or electronic form, either:

115

116 a) assurance in the form of a general disclaimer to the effect that such party does not hold  
117 and does not currently intend holding any essential patent claim(s); or

118

119 b) assurance that a license to such essential patent claim(s) will be made available to  
120 applicants desiring to utilize the license for the purpose of complying with the guidance  
121 or requirements in this ITL draft publication either:

122

123 i. under reasonable terms and conditions that are demonstrably free of any unfair  
124 discrimination; or

125

126 ii. without compensation and under reasonable terms and conditions that are  
127 demonstrably free of any unfair discrimination.

127

128 Such assurance shall indicate that the patent holder (or third party authorized to make assurances  
129 on its behalf) will include in any documents transferring ownership of patents subject to the  
130 assurance, provisions sufficient to ensure that the commitments in the assurance are binding on  
131 the transferee, and that the transferee will similarly include appropriate provisions in the event of  
132 future transfers with the goal of binding each successor-in-interest.

133

134 The assurance shall also indicate that it is intended to be binding on successors-in-interest  
135 regardless of whether such provisions are included in the relevant transfer documents.

136

137 Such statements should be addressed to: [nistir-8356-comments@nist.gov](mailto:nistir-8356-comments@nist.gov)

138

139

140 **Table of Contents**

141 **1 Introduction ..... 1**

142 **2 Definition of Digital Twins ..... 2**

143 **3 Motivation and Vision ..... 4**

144 3.1 Advantages of Digital Twin Technology ..... 4

145 3.2 Expectation of Standards ..... 5

146 3.3 A More Detailed Look at Supportive Technologies ..... 5

147 **4 Operations on Digital Twins ..... 7**

148 4.1 Creation and Definition of Digital Twins ..... 7

149 4.2 Manipulation and Modification of Digital Twin Definitions ..... 8

150 4.3 Exchange of Digital Twin Definitions ..... 8

151 **5 Usage Scenarios for Digital Twins ..... 9**

152 5.1 Viewing Static Models of Digital Twins ..... 9

153 5.2 Executing and Viewing Dynamic Models of Digital Twins ..... 9

154 5.3 Real-time Monitoring of Real-world Entities ..... 11

155 5.4 Real-time Command and Control of Real-world Entities ..... 12

156 **6 Highlighted Use Cases ..... 13**

157 **7 Cybersecurity Considerations ..... 14**

158 7.1 Novel Cybersecurity Challenges ..... 14

159 7.1.1 Massive Instrumentation of Objects ..... 14

160 7.1.2 Centralization of Object Measurements ..... 15

161 7.1.3 Visualization/Representation of Object Operation ..... 15

162 7.1.4 Remote Control of Objects ..... 15

163 7.1.5 Standards for Digital Twin Definitions ..... 16

164 7.2 Traditional Cybersecurity Challenges and Tools ..... 16

165 **8 Trust Considerations ..... 18**

166 **9 Conclusions ..... 22**

167 **References ..... 23**

168 **List of Appendices**

169

170 **Appendix A— Glossary ..... 26**

171 **Appendix B— Acronyms ..... 27**

172

**1 Introduction**

174 Digital twin (DT) technology is an emerging field that needs additional definitional clarity as  
175 well as an analysis of cybersecurity and trust considerations. As with many new technologies,  
176 digital twins are in that initial period of flux characterized by a healthy dose of evolution,  
177 discussion, and confusion regarding what a digital twin really is—or should be—and what its full  
178 scope and applicability will be.

179 Digital twin technology enables the creation of electronic representations of real-world entities  
180 and the viewing of the state of those entities. These entities can be either physical or perceived  
181 (e.g., processes). The digital facsimiles can represent entities to be constructed or existing  
182 entities. With existing entities, the copies can be static (representing a point in time) or dynamic  
183 (linked to an entity and continuously updated). Dynamic twins can be used to control their linked  
184 objects. Twins can be instrumented to test their functionality and utility. Multiple digital twins  
185 can be composed, and the composition of twins can be tested.

186 As with many new information technologies, it uses many existing foundational technologies  
187 and in many cases appears similar to existing capabilities. It covers what exists today in modeling  
188 and simulation but then casts a broader vision for what could be. Standards will play a significant  
189 role as the full digital twin vision will not be possible without interoperable digital twin  
190 definitions and tools. Particularly important in this space are considerations for digital twin  
191 cybersecurity and trust. For any new digital technology, cybersecurity and trust should be  
192 addressed early. Digital twin technology is no exception; this is especially true for nascent  
193 standards efforts that seek to define and structure the technology.

194 This report provides an introduction to digital twin technology, to provide clarity on what it  
195 really is and how it expands on current capabilities. It explains the important components and  
196 functions, and then discusses cybersecurity and trust considerations. It begins with a section  
197 defining digital twins followed by a section providing the motivation for using digital twin  
198 technology. This is followed by a discussion on typical operations performed on digital twins  
199 and then an explanation of technical usage scenarios. It then provides example applications of  
200 digital twin technology in industry. Having given the reader a high-level understanding of digital  
201 twin technology, the report then explores cybersecurity considerations. It identifies and explores  
202 novel cybersecurity challenges related to digital twins. It also discusses traditional cybersecurity  
203 needs and approaches that apply to digital twin systems. Lastly, it discusses trust issues that can  
204 inhibit a digital twin implementation from providing the desired operational functionality with an  
205 acceptable level of quality. These last two discussions of traditional cybersecurity and trust  
206 considerations are conducted in the context of existing NIST guidance and documents.

207

## 208 **2 Definition of Digital Twins**

209 Currently, there are several unofficial “definitions” for digital twins—some created by  
210 researchers, some by standards committees and consortia, some by industry, and still others that  
211 are implicitly suggested by commercial enterprises that make statements that their software  
212 applications are “digital twin-compliant” in spite of the absence of any agreed-upon definition or  
213 consensus of vision for digital twins [1].

214 Despite today’s nebulous understanding and lack of formal definition of what digital twins really  
215 are—or will eventually become—the definition of a digital twin used in this paper is:

216 *A digital twin is the electronic representation—the digital representation—of a*  
217 *real-world entity, concept, or notion, either physical or perceived.*

218 In practice, a digital twin will consist of a definition that will be created and persist in a digital  
219 computer environment. Computer software applications will read digital twin definitions to  
220 present a human user with a virtual view of the real-world object represented by the digital twin.

221 The use of the term *virtual* is appropriate here. A common theme that is part of every  
222 conversation or unofficial definition of digital twins is that software applications will typically  
223 present for the benefit of a human user a visual graphic representation, either static or dynamic,  
224 of a real-world object via the object’s digital twin. Many of these real-world entities will be  
225 things that are commonly recognized as having physical form, such as an aircraft engine, an oil  
226 derrick, a valve in an oil pipeline pumping station, a bicycle, or a human heart.

227 However, according to the definition of digital twins given above, an entity represented by a  
228 digital twin can also be something abstract. The following definition of *abstract* from the  
229 Merriam-Webster online dictionary is appropriate for a discussion of the various types of entities  
230 that a digital twin can represent:

231 **abstract:** noun: *expressing a quality apart from an object* [2]

232 In this context, a digital twin could represent a real-world entity that is neither concrete nor  
233 physical in the traditional sense of these words. That is, the digital twin could represent  
234 something that is certainly real in the sense that it is perceived by a human being as something  
235 that truly exists—it just does not have an identifiable physical form in the traditional sense.

236 A good example of such an entity that is real but is without traditional physical form or  
237 manifestation is a *process*. For instance, a *process* in a computer operating system is certainly  
238 real, but it is quite different from the typical entity that one would normally think of as physical.  
239 Our cognitive human perception tells us that the computer process is indeed real; one can clearly  
240 observe the effects it has on other objects, such as the disk drives in a computer. However, its  
241 nature as a concrete, tangible, physical entity is not so obvious.

242 The computer operating system process itself is really a conglomeration of other intangible  
243 things, such as electrical signals, the states of registers containing voltage and current levels, the

244 electrical state of memory, and so forth. To further complicate matters, one can view these  
245 register states and electrical signals as representing the running computer program. The program  
246 itself is an abstract entity. Its physical form, residing as a magnetic state on a hard disk, is  
247 certainly not the notion one has of the program when looking at its graphical user interface.  
248 Likewise, the programmer's view of the source code or the breakpointed state of the program in  
249 a debugger are quite different manifestations from the magnetic state of sectors that store the  
250 program on a hard disk drive. Nonetheless, one can think of a computer program—either  
251 statically or dynamically—as something real.

252 *A business process* is another example of a process and a very abstract entity that is certainly real  
253 to a human, albeit not so material. Yet one could define a digital twin to represent a business  
254 process. In fact, software exists today to do just that.

255 *A manufacturing process* is yet another example. Chemists and chemical engineers define  
256 processes to produce compounds and chemicals, as well as facilitate material processing, such as  
257 oil refining or the production of nuclear fuel. A chemist could describe such a process using  
258 pencil and paper, or a digital twin could describe it, its steps, or a simulation of every aspect of  
259 the dynamic execution of such a process in a factory or chemical plant. Clearly, these processes  
260 are real.

261 The notion of a process described above is certainly not the only type of abstraction that digital  
262 twins can represent. As stated previously, a digital twin can represent anything that a human can  
263 conceive or perceive, whether real or not, material or not, or physical or not—basically, any  
264 abstraction.

265 For example, astrophysicists and cosmologists have postulated the existence of black holes, but  
266 none are known to exist. Nevertheless, scientists have created both static and dynamic models of  
267 black holes, and these models include the characteristics and dynamic behavior of black holes  
268 according to theory and the mathematical equations that attempt to describe their static and  
269 dynamic nature. Such a model could be built via a digital twin and used by computer programs to  
270 present humans with static views and dynamic simulations of the behavior of a black hole.

## 271 **3 Motivation and Vision**

272 Nothing in our definition of digital twin technology is new; it has all existed in one form or  
273 another. The use of computers and software to represent entities and simulate dynamic behavior  
274 has existed since the first computers. Engineers use software to design, simulate, and verify  
275 amusement park roller coasters, bridges in high winds, buildings in earthquakes, and the  
276 aerodynamics of aircraft.

277 However, this does not mean that digital twin technology is just a repackaging and renaming of  
278 existing technology. The focus on, and interest in, digital twins is due to the maturation of  
279 multiple underlying technologies that is making it possible to apply simulation and modeling, in  
280 the form of creating digital representations, much more broadly and make it accessible to a much  
281 wider user base. The emergence, through the Internet of Things (IoT) revolution, of small low-  
282 cost battery powered sensors that are network connected has enabled massive sensor deployment  
283 to a wide variety of objects (e.g., modern buildings may have thousands of sensors). These  
284 sensors then provide information that can feed and maintain complex models of those objects.  
285 The advances in powerful but low-cost processing and storage enable us to maintain, view, and  
286 manipulate these digital replicas without having to use special purpose expensive hardware. And  
287 finally, the recent advances in virtual reality (VR) and augmented reality (AR) have enabled  
288 inexpensive visual viewing of digital twin representations.

289 Whether or not these developments catalyze digital twin technology into widespread use may  
290 depend upon work in standards development. Currently most IoT systems, simulation and  
291 modeling software, and VR and AR systems exist in stovepipe proprietary systems. It is possible  
292 to combine them, but it takes significant work to integrate them. Much of the work in the  
293 emerging digital twin area is in the creation of protocols and standards to enable plug and play  
294 integration. The idea is to mix and match and be able to use any viewer with any digital twin  
295 simulator and modeler along with any sensing device. The idea is to be able to load any digital  
296 twin computer file into a digital twin system and have it function regardless of what is being  
297 modeled. These are lofty goals for the emerging digital twin community; their success in  
298 standards may largely determine the extent to which the technology is used.

### 299 **3.1 Advantages of Digital Twin Technology**

300 Creating a platform or mechanism that supports the creation of digital models of real-world  
301 objects is advantageous for several reasons. One major motivation is that one can study the  
302 object via its model prior to building the real-world version. This practice can reduce certain  
303 types of risk. This advantage increases when multiple entities are modeling different objects that  
304 need to work together. If cooperating entities can share digital twin definitions, then they can  
305 more easily model and simulate object interactions digitally prior to the realization of the output  
306 product.

307 In fact, this is the case today in select industries; it is simply not widely deployed and done in  
308 proprietary systems. All manner of real-world objects is conceived, described, modeled, and  
309 designed on the computer, from electrical circuits, integrated circuits, and amusement park rides  
310 to bridges, oil derricks, aircraft, power plants, and nuclear reactors. All of the engineering

311 analysis is also performed on a computer prior to building anything physical. The software  
312 applications employed to do this work contain dynamic 2D and 3D graphics to visually represent  
313 everything from the interaction of atoms and molecules in chemical and biological reactions to  
314 fatigue and flutter in aerodynamic structures.

### 315 **3.2 Expectation of Standards**

316 The adoption of standards and the adherence to standards by the systems built around them may  
317 ensure interoperability, compatibility, safety, and cybersecurity. Moreover, the assurance that  
318 software and hardware systems, tools, and applications adhere to and properly implement  
319 standards engenders credibility and trust [3]. However, no digital twin specific standard currently  
320 exists (although certainly digital twin implementations can leverage many generic information  
321 technology standards). When such standards do exist, there may be multiple cooperating (or  
322 competing) ones. Rarely does a single standard adequately address everyone’s needs. In this  
323 case, there must be some synergy such as that realized by either harmonization or standards  
324 blending [4]. In the standards blending approach, each standard—in fact, each functional area of  
325 each standard—will still need to be vetted. Tool vendors, software and hardware application  
326 vendors, and users can be compliant with all standards by ensuring that they use only vetted  
327 elements. Using this approach should lead to the interoperability of tools and applications.

328 Additionally, for standards to work they would need to cover each involved business domain.  
329 Everyone operating in the digital twin ecosystem in specific business domains would need  
330 standards and standards-based products that adhere to a common set of business processes and  
331 use cases such that interoperability can be achieved in the business domain. It is not enough to  
332 have standards just to enable interoperability in the purely technology domain.

### 333 **3.3 A More Detailed Look at Supportive Technologies**

334 This section discusses in more detail two of the supportive technologies undergirding the recent  
335 interest in digital twin technology: VR/AR and IoT.

336 One will frequently encounter VR and AR in digital twin discussions online and in the opus of  
337 digital twin-related publications and articles. One of the visions for digital twins is to leverage  
338 VR and AR to create the enhanced user interfaces and user experiences for human beings to  
339 comprehend complex entities. Humans rely heavily on visual sensory input, and VR and AR  
340 promise to help describe real-world entities through the models created for them.

341 IoT is also often referenced in digital twin discussions and literature because of the recent  
342 advances in sensors and sensing. There is both a significant advance the creation of sensors of all  
343 kinds while there is also an ongoing, dramatic proliferation of such sensors being put into  
344 operation. These sensors are typically network connected and drive the ability of twins to model  
345 real world objects in ways that were not possible until recently.

346 IoT is often used to create what is referred to as an information fabric or “network.” This fabric  
347 encompasses more than just the sensors although the sensors are obviously the central  
348 component. An IoT fabric consists of the observed entities, the sensors that observe and gather  
349 information, the connectivity elements, the processing components (i.e., what one might think of

350 as “the back-end compute servers”), and the components that process the IoT data.

351 With these new sensors being deployed on an IoT fabric, digital twins can represent (and  
352 dynamically maintain the representation of) an instance of an instrumented object [5]. Thus, the  
353 application of digital twins goes beyond simply modeling a class of real-world entities; it can  
354 also be used to represent and track a specific object, maintain the real-time status, and present a  
355 dynamically updated view to a user. The digital twin model may also be manipulated by a user to  
356 control the actual object. This is where digital twin technology may advance beyond traditional  
357 modeling and simulation software.

## 358 **4 Operations on Digital Twins**

359 In an effort to provide a full overview of digital twin technology, this section discusses lower  
360 level operations that are performed on digital twins:

- 361 • Definition of digital twins and the creation of digital twin electronic artifacts
- 362 • Manipulation and modification of electronic digital twin definitions
- 363 • Exchange via electronic communications of digital twin artifacts

364 Note that these are operations typically performed on electronic assets; we discuss here how they  
365 apply to digital twins and any special considerations.

### 366 **4.1 Creation and Definition of Digital Twins**

367 A digital twin *definition* is really a *formal description* of the real-world twin—the real-world  
368 entity—that the digital twin represents. The starting point for all activity involving digital twin  
369 technology is the creation and persistence of digital twin definitions as digital artifacts by  
370 computer software applications. These artifacts can represent both static and dynamic models of  
371 the real-world entities that correspond to their respective digital twin.

372 Since there is currently no digital twin standards definition, there is no formalization of a digital  
373 twin definitions at this time. The type of digital twin defined will dictate the precise makeup of  
374 the definition files. For example, there is no requirement that a given digital twin definition  
375 include a dynamic view of its real-world counterpart; it could comprise only a static view of the  
376 object, if so desired. Thus, not all digital twin definitions will necessarily contain all possible  
377 declarations or definition constructs defined in some future standard. Similarly, not all hypertext  
378 markup language (HTML) files utilize all tags defined by the HTML standard [6].

379 If the digital twin represents only a static model of an entity, there would be no dynamic  
380 information, such as how to render animation, video, or dynamic graphics. Consider, for  
381 example, a VR presentation of a naval vessel. A static view could represent the internals of the  
382 ship seen through VR as if a person was conducting a literal walk-through of the vessel. VR  
383 technology would be more amenable to this application than a 3D PDF view. The latter would  
384 comprise detailed engineering drawings tantamount to an architect's blueprint drawings.  
385 However, it would be difficult to present the equivalent of what a person would see walking  
386 through the interior of the ship. A digital twin creates a model of the object it represents, not just  
387 a particular view. It can present whatever view and viewpoint of the real-world entity that the  
388 author desires.

389 A digital twin definition can contain as much or as little information about its real-world  
390 counterpart as its authors desire. The breadth, scope, degree of granularity, and detail are  
391 completely the decision of the creators. As with other models, the *nature* of the real-world object  
392 and its digital twin's presentation of it are independent of the scope, extent, granularity, and level  
393 of detail contained in the digital twin definition. The main consideration is that all aspects of the  
394 model created by the digital twin—nature, scope, granularity, and level of detail—should be  
395 suitable for the intended application of the digital twin definition.

396 A practical consideration is the digital twin definition authoring itself. While it might very well  
397 be possible to author definitions using a text editor, this practice could become supplanted by  
398 tools. This is similar to how not many people hand-code HTML or XML anymore [7]. The  
399 complexity of digital twin definitions could even preclude the ability to craft definitions by hand.

400 In industries such as aerospace, civil engineering, mechanical engineering, and heavy  
401 construction, designers, modelers, and engineers use sophisticated software applications to create  
402 digital artifacts that represent what they plan to build, including aircrafts, bridges, buildings,  
403 amusement park rides, dams, tunnels, cranes, oil rigs, and a plethora of other things. Some of  
404 these software applications support the writing, persistence, and “export” of their artifacts in  
405 standard file formats and encodings, such as the 3D PDF standard [8]. However, the majority of  
406 these applications use their own completely proprietary file formats and encodings to define,  
407 capture, and persist the models, drawings, and various artifacts that they can create.

408 Standards will be important here. Like existing commercial applications, any future digital twin  
409 standard may include a *language* for describing and defining digital twins. Such a language, like  
410 any other language, would consist of a *formal grammar*, *syntax*, and *semantics*. It would have to  
411 be comprehensive enough—both general and specific—to support the definition of artifacts to  
412 represent any arbitrary real-world entity that a digital twin can represent [5]. Most likely, a  
413 standard would accommodate the creation of 2D, 3D, VR, and AR models, both static and  
414 dynamic, for visual presentation to human users. It might also accommodate the creation,  
415 manipulation, and persistence of presentation forms that might not be human-comprehensible  
416 (i.e., presentations intended for machine consumption).

#### 417 **4.2 Manipulation and Modification of Digital Twin Definitions**

418 Once a digital twin definition exists, it will be available for viewing (reading), modification  
419 (editing), resaving modifications, and duplication. This refers to the review or viewing of the  
420 definition itself, not the viewing of the *presentation* of the digital twin’s model of the real-world  
421 entity that it describes.

422 If standards are developed, industry may develop “what-you-see-is-what-you-get” (WYSIWYG)  
423 editors and tools to complement the standard text editors that exist, which include stand-alone  
424 editors as well as interactive developer environment (IDE) tools. Such a tool would comprehend  
425 the digital twin definition language and its file formats, encodings, grammar, syntax, and  
426 semantics. This would enable the tool to correctly read a digital twin definition in order to  
427 support its review or modification by a human user. This is no different than the need for a  
428 WYSIWYG HTML editor to comprehend how to properly produce formatted HTML source.

#### 429 **4.3 Exchange of Digital Twin Definitions**

430 Digital twin definitions are simply computer files that are available for reading, writing,  
431 execution, and general manipulation. They can be sent to recipients for use, similar to how 3D  
432 printer files are shared to enable many people to create the same object. The power in sharing  
433 these files is that they follow a standard. Such standards will need to be developed for digital  
434 twin technology to harness this advantage as current systems use proprietary formats.

## 435 **5 Usage Scenarios for Digital Twins**

436 This section describes scenarios that are likely to represent the main general categories of usage  
437 of digital twins in practice. The broad categories of application for digital twins are:

- 438 • Viewing static models
- 439 • Executing and viewing dynamic simulation models
- 440 • Streaming execution of dynamic simulations
- 441 • Real-time monitoring of real-world entities
- 442 • Real-time command and control of real-world entities

### 443 **5.1 Viewing Static Models of Digital Twins**

444 This section describes the viewing of static digital twins. This type of view presents a non-  
445 changing model of a real-world twin, regardless of the nature of the real-world entity and  
446 regardless of how that entity may change over time. The real-world entity may not even exist yet  
447 as would occur during the initial design of an object. Such a model would only be suitable for  
448 examining the nature of an object at a point in time. Static descriptions do not model an object's  
449 behavior [11].

450 Examples include a computer numerical control (CNC) milling machine using a static 3D model  
451 to describe the object to be milled. In the aerospace industry, designers or modelers first create  
452 what they call a *solids model* of the component or entity that they are designing. These comprise  
453 static 2D or 3D views of a component, such as an aircraft wing or empennage (tail assembly). A  
454 building architect creates drawings of a house to be built. Typically, the architect creates various  
455 2D views, such as a site plan, floor plan, and elevation plans. Architects could adopt the practice  
456 of creating 3D views, but these would be less useful to building contractors, and they are more  
457 difficult to read. The creator of the model can define it as they see fit for the intended use, and  
458 the data in the model can be used to create a suitable view.

### 459 **5.2 Executing and Viewing Dynamic Models of Digital Twins**

460 This section describes scenarios in which a human user executes a digital twin definition to  
461 model an object's changes over time and views the dynamic changes to the object. As with the  
462 static viewing, the object may or may not yet exist. A dynamic model presents a *simulation* of  
463 the *operation* or *dynamic behavior* of a real-world entity or object; it describes how an object  
464 changes as measured via one or more metrics that represent one or more aspects or  
465 characteristics of the object [12].

466 Some examples are the visual updates to graphics that show how the scaffolding or track of a  
467 roller coaster bends as a function of applied force from wind loading or from the traveling  
468 toboggan, the dynamic response of a building—how the building moves—in an earthquake, or  
469 how an aircraft's wing bends under changing loads in flight.

470 Dynamic modeling, simulation, and presentation (display) are quite different from the static  
471 modeling and visual presentation of objects discussed in the previous section. An engineer who

472 wants to understand how the milled block mentioned above changes in malleability, ductility, or  
473 tensile strength over time as it is heated at some rate would need a dynamic model that includes a  
474 knowledge of thermodynamics, mechanical engineering, and materials engineering. That is, a  
475 dynamic model shows more than just the static dimensions or information about the shape,  
476 material, or density of an object.

477 For the aerospace engineer, a static model is adequate to show the material or dimensions of a  
478 component, such as a wing assembly. However, one needs a dynamic model to analyze how the  
479 wing performs dynamically in a wind tunnel or in flight and to understand materials stress, fluid  
480 dynamics, and dynamics (e.g., natural frequency, normal modes, and flutter).

481 In dynamic modeling, simulation software applications update their model and view at some  
482 rapid frequency that represents real-time or near real-time behavior. A dynamic display should  
483 be updated at a frame rate that ensures smooth motion, such as 24 frames per second or higher.

484 Although most engineers would envision a graphical user interface when one mentions dynamic  
485 simulation and modeling, the presentation—the MVC *presentation or view*—need not be  
486 graphical. It could be a table of numbers displayed on the user’s console or written to a file. The  
487 numbers could represent the change in some aspect of the object according to a suitable metric,  
488 which may not be user-friendly but is a presentation of the model, nonetheless.

489 A visual presentation can use many methods to create a more comprehensible presentation. For  
490 example, a visual presentation of a wing in flight could include the use of various colors to show  
491 the variability of stress along the wing’s surface area with the application of force. The choice is  
492 up to the author of the model and its views, all of which represent the dynamic nature of the  
493 object being simulated.

494 The various types of presentation of dynamic simulations that digital twin technology may  
495 support can be categorized as:

- 496 • Real-time or near real-time presentation of a simulation during the simulation run
- 497 (execution of the dynamic simulation model)
- 498 • Local playback of a previously recorded simulation run
- 499 • Streaming of a dynamic simulation run
- 500 • Download and local playback of a previously recorded simulation run

501 The *imperative* and *declarative* programming paradigms are both important for the kinds of  
502 software applications that will use digital twin technology. Think of the MIT X Window System,  
503 which represents the *imperative programming paradigm* to display graphics [15]. Applications  
504 make calls to X library routines (and those of the graphics toolkits built atop the venerable `Xlib`  
505 and `Xt` X Window System libraries). Those calls draw the graphics, and the X display server  
506 renders the visual graphics on the graphics display [16].

507 In the *declarative programming paradigm*, the information encoded indicates *what* is to be  
508 displayed rather than *how* to do it [17]. There are no imperative calls to execute the steps to  
509 present (display) the graphics. HTML is an example of a declarative programming paradigm. An

510 HTML file represents directives of *what* to display, not *how* to display it; there are no imperative  
511 commands to display the content like the programmatic calls to routines in the X Window  
512 System libraries.

513 The streamed or downloaded *content* that represents digital twin dynamic simulations could  
514 consist of pre-captured video, such as an MPEG-encoded video. In this case, the digital twin  
515 application software probably creates the standard video from the simulation run.

516 Alternatively, digital twin software applications could create declarative-style content to be  
517 parsed, comprehended, and manipulated for display by the client receiving the content. This  
518 might look something like HTML from an architecture viewpoint. The content would consist of  
519 a combination of declarative constructs, including some to point to other content such as pre-  
520 captured or pre-recorded video or even executable code that is in the imperative style. Web pages  
521 today contain directives to download executable code, such as JavaScript, that are executable  
522 programs.

### 523 **5.3 Real-time Monitoring of Real-world Entities**

524 This section describes monitoring the state or condition of real objects. Monitoring is  
525 fundamentally different from simulation. Monitoring collects the information—typically in real-  
526 time or near real-time—of actual real-world entities. There is no simulation or emulation at all.

527 A tangible example would be the real-time monitoring of the state of an aircraft’s wing in flight  
528 (e.g., in a wind tunnel, on a test bench, or in real flight on a real aircraft). The monitoring could  
529 capture information about anything, such as measuring materials stress or fatigue, aerodynamic  
530 drag, or laminar flow.

531 Typically, monitoring will involve the use of sensors to gather the data to be used to construct a  
532 view of the state of the real-world entity being monitored. Today, the term “sensor” may  
533 immediately bring to mind the “Internet of Things” (IoT) [18], but the terminology is an  
534 unnecessary distraction. Conceptually, a sensor can exist anywhere. It can be on the object being  
535 observed and monitored, or it can be physically remote. For example, satellites now have sensors  
536 that perform ground imaging. Upon gathering data that represents some aspect of the object’s  
537 state or condition, sensors send the collected data to software systems. The system could be local  
538 or remote, and remote connections could be wired or wireless. They could also use any of a  
539 number of transmission mediums, technologies, and protocols.

540 These systems are not new. Airline operations centers have been monitoring their aircraft in-  
541 flight for years. The vision for digital twins is to use this monitoring data to create a dynamically  
542 updated digital replica and to, through standards [19], enable the interoperability of different  
543 tools to view and manipulate the digital replica. This could enable, for example, an operator to  
544 take a current digital replica of an aircraft and manipulate it to apply artificial stressors to  
545 calculate how that particular airplane in its lifecycle and with its specific operating parameters  
546 can handle unexpected events.

547 Monitoring can be real-time or in near real-time. A typical jet engine has numerous sensors that  
548 monitor every imaginable aspect of the engine's parts and operations. The data gathered by the  
549 sensors can be transmitted to applications that present 3D graphics or VR or AR experiences to  
550 users. An airline mechanic can use a VR system to view an operating engine in flight as if they  
551 were standing in the engine to examine a particular part.

#### 552 **5.4 Real-time Command and Control of Real-world Entities**

553 Real-time links to a real-world object create an opportunity for yet another usage scenario,  
554 namely command and control via a digital twin platform. Command and control systems require  
555 bidirectional links and the transmission of information. The digital twin platform is amenable to  
556 presenting a view of the object or objects associated with their digital twins. However, the  
557 software systems built around the digital twin cornerstone can command the observed objects,  
558 such as an oil well drill, deep sea exploration vessel, unmanned aerial vehicle (UAV), satellite,  
559 or spacecraft.

560 Sensors and communications mechanisms collect and send status information to the main  
561 control. The main system will most likely present the object's status to a human user, although  
562 this is not required. In response to some evaluation, assessment, or processing of the status  
563 information, commands are sent back to the object to modify its state or command it to do  
564 something.

565 This kind of bidirectional command, control, and communications is not new. The difference  
566 with digital twin technology is the detailed digital representation of the controlled object that is  
567 itself a model of the object (not just information feeds about the object). Also, digital twin  
568 standards may enable interoperability between tools and formats to enable this control. For  
569 example, applications may not need to use proprietary schemes for defining and controlling  
570 objects and representing models, views, and other aspects, such as semantics, syntax, file  
571 formats, and tools.

**6 Highlighted Use Cases**

573 This section presents a few sample applications of digital twins to prepare the reader for the  
574 subsequent discussion of the potential cybersecurity vulnerabilities of digital twin environments  
575 and ecosystems. The examples in this section are taken from industries that are already exploring  
576 and using digital twin technology.

577 **Unmanned aerial vehicles (drones):** The unmanned aerial vehicle (UAV) or drone is used in  
578 environmental monitoring. UAVs come in all sizes, shapes, configurations, and sophistication.  
579 The more advanced drones can operate either autonomously or via the control of a human sitting  
580 in a command and control center miles away from the UAV's physical location. In the case of  
581 UAVs that are operated and controlled remotely, the operator has a user interface that gives real-  
582 time status on many aspects of the UAV's state and condition.

583 **Ocean-going supertankers:** Digital twin systems could be used at every life stage of various  
584 ocean-going vessels, from naval vessels to commercial supertankers. During construction, digital  
585 twins could be used to construct 2D or 3D static views or VR/AR views of the vessel. Such VR  
586 or AR views would enable architects, designers, engineers, and maintenance crews to "see" the  
587 vessel as if they were physically walking through it. During operations, digital twin technology  
588 would enable operators and crewmembers to monitor every aspect of the ship, from its propeller  
589 screws and drive shafts to the engine room, providing views to someone on the ship's bridge—  
590 possibly precluding the need for certain physical monitoring and inspection.

591 **Oil derricks and ocean drilling platforms:** Oil derricks drill for oil in some of the most  
592 inhospitable and potentially treacherous environments. Sometimes, they drill down to great  
593 depths below the ocean's surface. Systems built around digital twins could enable designers,  
594 engineers, and operators to form a model and visual representation of the oil rig, drill rig, and  
595 drill bit head deep down in the ocean.

596 **Telemedicine and remote patient monitoring:** There are currently systems that remotely  
597 monitor certain parameters of a patient's health. One system places a wireless communications  
598 and sensor apparatus under the patient's bed, monitoring the signals sent by the patient's  
599 pacemaker and sending the data to a doctor or hospital.

600 **Robotic surgery:** There are surgical robots that perform various kinds of surgery. Some require  
601 an actual human surgeon to control the robot, but others require only a human surgeon to  
602 monitor the robot's automatic execution of the surgery. Future systems built around standards  
603 based digital twin technology could enable interoperability. For instance, one company's surgical  
604 robot could be able to interoperate with another company's VR system that specializes in the  
605 representation of human organs.

## 606 **7 Cybersecurity Considerations**

607 New trends in computing may appear to be little more than a simple rebranding of existing  
608 technology, such as cloud computing and big data. However, a closer inspection can reveal that  
609 the integration of known components combined with a certain maturation in the industry has  
610 created novel characteristics and features, and these new capabilities often come with unique  
611 cybersecurity challenges that did not necessarily exist for each of the component pieces. These  
612 challenges may then require novel cybersecurity approaches or a new application of traditional  
613 cybersecurity techniques. That said, the traditional cybersecurity necessary for each individual  
614 component is almost always still necessary in the aggregated technology.

615 Digital twin technology is no different. The components of digital twin technology (e.g.,  
616 instrumented devices, aggregated metrics, visualization, and remote control) are not new.  
617 However, in the aggregate, it may enable a new and powerful paradigm. This section will  
618 explore what is new in digital twin technology from a cybersecurity perspective, what challenges  
619 these new features present, how they might be secured, and how traditional cybersecurity  
620 approaches still apply to the individual components and mechanisms that make up digital twin  
621 technology.

### 622 **7.1 Novel Cybersecurity Challenges**

623 Digital twin technology has at least five novel features that require special cybersecurity  
624 considerations:

- 625 1. Massive instrumentation of objects (usually using IoT technology)
- 626 2. Centralization of object measurements into digital twin definitions
- 627 3. Visualization/representation of object operation through digital twin definitions
- 628 4. Remote control of objects through manipulation of digital twin definitions
- 629 5. Standards for digital twin definitions that allow for universal access and control

630 This list is not necessarily exhaustive, and additional novel cybersecurity challenges will  
631 indubitably arise as digital twin technology matures.

#### 632 **7.1.1 Massive Instrumentation of Objects**

633 Advances in IoT technology have provided a wide variety of cheap and network-connected  
634 sensors that can be used to instrument objects. This instrumentation can then feed digital twin  
635 definitions, enabling the modeling of real-world objects and real time monitoring (and possibly  
636 remote control) of many objects to a fine level of granularity. This monitoring will likely be done  
637 with inexpensive, network connected IoT sensors. These sensors may have vulnerabilities as well  
638 as limited computing capacity, network throughput, power, and upgrade potential. This has  
639 cybersecurity significance because the detailed innerworkings of real-world objects would be  
640 revealed (and possibly controlled) via the digital sphere. Previously, such objects were protected  
641 from digital interference because they were not digitally instrumented. All of that would change  
642 with digital twin instrumented objects (e.g., ‘smart’ homes, ‘smart’ buildings, and ‘smart’ cities).

### 643 **7.1.2 Centralization of Object Measurements**

644 This massive instrumentation of objects could provide a malicious entity visibility into (and  
645 perhaps control over) the detailed inner workings of an object through the compromise of the  
646 sensors. However, each sensor or controller is a separate IoT device. The sheer number and  
647 distribution of them could inhibit a malicious entity from completely taking control of the  
648 instrumented physical object. However, digital twin technology involves centralizing the data  
649 and control feeds from the massive instrumentation of an object. This creates great efficiency in  
650 simulation, modeling, and control, but it also centralizes sensitive data and control interfaces. If  
651 the digital twin definition is hacked, the attacker has total access to all data about the  
652 instrumented object.

### 653 **7.1.3 Visualization/Representation of Object Operation**

654 An attacker with control of the digital twin definition and instrumented object data could  
655 manipulate how the object is presented to the users of the digital twin definition. There is heavy  
656 emphasis in digital twin technology on VR and AR. Control of the digital twin definition enables  
657 manipulation of the reality presented to the human operator. The design of an object to be built  
658 could appear to be correct when in reality the attacker has redesigned it with flaws. The status of  
659 a monitored object could be changed to cause an operator to take action that would then damage  
660 the object or the people and things around the object. A remotely controlled digital twin object  
661 could be manipulated by an attacker while the visualization to the user hides any changes.

662 Since a digital twin definition can present its related object's state through more than just  
663 visualization to a human, digital twin definitions could be designed to present object  
664 representations to other consuming digital systems, including other digital twin definitions.  
665 Digital twin definitions may be built on top of one another following an object-oriented  
666 programming (OOP) model. They may also use an object representation from another digital  
667 twin definition to model objects that have some linkage (be it physical or virtual). The  
668 manipulation of a digital twin representation can then deceive or corrupt related digital twin  
669 definitions and other digital systems consuming the digital twin definition's object  
670 representation.

### 671 **7.1.4 Remote Control of Objects**

672 A goal of digital twin technology is to have a detailed simulation of an object through extensive  
673 instrumentation and use that simulation to remotely control the object. Remote control  
674 technology has long existed for many types of objects; what is different here is the goal of  
675 building a digital facsimile that is constantly updated and to add controls to the digital  
676 representation while having the effects transmitted to the controlled object.

677 A hacked digital twin definition would then not only provide an attacker access to the raw  
678 remote-control mechanisms but also to a real-time, updated, digital facsimile with possibly  
679 higher level of abstraction control mechanisms. These higher-level controls would be easier to  
680 understand and use. The attacker could manipulate these controls at the digital twin definition  
681 level or at the level of the raw remote-control signals while deceiving any human operator by

682 presenting a false digital facsimile. This could deceive the user who is relying on the provided  
683 digital facsimile rather than the individual raw metrics from the instrumented object.

#### 684 **7.1.5 Standards for Digital Twin Definitions**

685 A significant push in the digital twin technology community is to create standards for digital  
686 twins that will be adopted by tools for digital twin definition creation, monitoring, linkage to  
687 monitored objects, and remote manipulation. This standardization push, if successful, would  
688 enable any standards-based tool to work with any digital twin definition. This is a significant  
689 factor in the excitement around digital twin technology because it could eliminate what are now  
690 proprietary silos of remote-controlled instrumentation.

691 Standardization, while beneficial in general, could aid attackers in subverting digital twins.  
692 Standardization in the IoT devices (and their communication protocols) used to instrument  
693 objects could make it easier for attackers to decipher measurements and send commands to the  
694 instrumentation. Standardization of the digital twin definition representation could enable an  
695 attacker to more easily subvert an existing definition or replace one altogether (e.g., with a  
696 malicious one created by the attacker). It could enable an attacker to more easily provide false  
697 visualizations to human operators. In summary, standardization could vastly reduce the learning  
698 curve for attackers to manipulate digital twin definitions by removing the unique proprietary  
699 measurement and control mechanisms that exist in many of today's remotely monitored and  
700 controlled objects.

701 Another possible scenario (that is similar to the problem today of malicious apps in app stores) is  
702 that of attackers creating useful looking but malicious digital twin definitions and providing  
703 them to the public. Digital twin standards would make it easy for anyone to understand how to  
704 write a digital twin definition and thus how to create a false one that might appear to be  
705 authentic. This is similar to phishers who create emails that look legitimate but lead users to  
706 malicious web pages. Once published, anyone with a standardized digital twin toolkit could then  
707 execute the malicious definitions.

#### 708 **7.2 Traditional Cybersecurity Challenges and Tools**

709 While the novel cybersecurity challenges of digital twin architectures have been the focus of  
710 attention so far, the components that make up digital twin technology have traditional  
711 cybersecurity challenges that must also be addressed. These challenges include the areas of  
712 confidentiality, integrity, availability, maintainability, reliability, and safety. This section reviews  
713 some of these needs as well as cybersecurity approaches commonly used to address them. This is  
714 not intended to be an exhaustive list but rather a sampling of important and obvious traditional  
715 cybersecurity that will need to be implemented. Any serious effort to secure a digital twin system  
716 should follow more exhaustive risk management guidance. For U.S. Government systems (also  
717 applicable to any system), this includes the NIST Risk Management Framework (RMF) [20].  
718 Critical to the cybersecurity of all systems is the NIST Cybersecurity Framework [21]; privacy  
719 controls are covered by the NIST Privacy Framework [22].

720 Digital twin technology focuses on the instrumentation and control of an object. Both the digital  
721 twin implementation and its instrumentation should have cybersecurity controls implemented  
722 and tested to protect against attack using a comprehensive cybersecurity control catalog (e.g.,  
723 using the previously referenced NIST Cybersecurity Framework [21] or NIST Special  
724 Publication 800-53, Rev. 5, *Security and Privacy Controls for Info Systems and Organizations*)  
725 [23]. For physical objects, IoT cybersecurity will be important as digital twin technology relies  
726 upon thorough instrumentation. IoT cybersecurity guidance can be found at the NIST  
727 Cybersecurity for IoT Program [24]. It will be important to ensure the cybersecurity of data in  
728 transit from IoT devices to the central digital twin definition repository. Public and standardized  
729 encryption algorithms should be used since proprietary encryption schemes can be weak and lack  
730 thorough vetting. The digital twin definition, its current state, and the collected data should be  
731 encrypted when not being actively used in order to achieve data at rest cybersecurity. Data  
732 governance policies and mechanisms must be in place to ensure that only the correct staff have  
733 access to the necessary data within a digital twin definition. Strong authentication mechanisms  
734 must then support this governance to ensure that the access policies are not subverted. This can  
735 include two-factor or multi-factor authentication as well as the use of hardware keys. The  
736 physical security of the digital twin system needs to be maintained since physical access is often  
737 sufficient to circumvent many digital security mechanisms. This includes both the IoT  
738 instrumentation of the monitored object as well as the hardware maintaining the digital twin  
739 facsimile.

740 The software and hardware used for digital twin definition maintenance and simulation should be  
741 designed and tested to be robust and fault-tolerant since failure could result in significant  
742 physical world consequences. This is especially true since standards will enable digital twin  
743 programs to work with any number of digital twin definitions, all of which will have differing  
744 sensitivities to faults and failures.

745 Lastly, the digital twin system (which covers the instrumentation, control/data channels, digital  
746 twin definition, and visualization/representation mechanisms) needs to be properly authorized by  
747 the appropriate organization officials as having sufficient cybersecurity given the risk tolerance  
748 of the system. In addition, a privacy analysis should be conducted, and privacy controls  
749 implemented based on a comprehensive privacy control catalog if the system contains any  
750 privacy-sensitive data (e.g., using the NIST Privacy Framework, Privacy Framework) [22].

751 One could argue that, in a specialized, secure environment, it is not necessary to have this level  
752 of cybersecurity in place. However, even the most secure networks usually have some  
753 connections to the outside world, even if not persistent (e.g., program updates through USB key  
754 transfers or the introduction of new hardware). It is best to plan cybersecurity based on a ‘zero  
755 trust’ model [25] where everything does its best to protect itself against everything else.

756

757 **8 Trust Considerations**

758 This section considers a set of 14 trust considerations that may need to be addressed to enhance  
759 the usefulness of digital twin technology. It is not directly focused on risk assessment and risk  
760 mitigation but rather on trust. That is, will digital twin technology provide the desired operational  
761 functionality with an acceptable level of quality? Answering this question begins with an  
762 understanding of trust. Here, trust is the probability that the intended behavior and the actual  
763 behavior are equivalent given a fixed context, fixed environment, and fixed point in time. Trust  
764 is viewed as a level of confidence. In this section, trust is considered at several levels: 1) Is the  
765 digital twin functionally equivalent to the physical object? 2) Can a specific digital twin be  
766 composed with another digital twin? 3) Is enough information available about the environment  
767 and context of the physical object? 4) Can digital twin technology be standardized to the point  
768 where certification of digital twins is possible?

- 769 1. **Digital Twin Creation Ordering:** The point in time at which a digital twin is created  
770 will have an impact on the correctness of the digital twin. For example, is it created  
771 before the physical object is created, or is it reverse-engineered from the physical entity  
772 (that it is intended to mirror)? Both approaches are valid. However, the fidelity of the  
773 digital twin may be reduced if it is created after the physical entity exists because there  
774 may be internal unknowns about the existing physical entity that cannot be discovered. A  
775 good analogy here is commercial off-the-shelf (COTS) software. Such products are black  
776 boxes—the source code is unavailable to the customer or integrator and, thus, hides  
777 internal syntax. For digital twin, this is a trust consideration.
- 778 2. **Temporal:** The digital twin paradigm has an implied temporal component to it,  
779 particularly since it deals with physical objects, and physical objects are bound by time.  
780 Hardware reliability theory and modeling states that physical objects, even when idle,  
781 suffer from levels of decay over time. For example, if a car has not been turned on for  
782 years, it is likely that the battery will be dead, and the car will not start. Physical objects  
783 will degrade and fatigue over time after usage. However, a digital twin will not degrade  
784 or fatigue over time. Therefore, at some point the physical and digital twins will be in  
785 conflict on some level. For example, a metal part could develop hairline fractures after  
786 usage that are not represented in the digital twin. This might suggest that the digital twin  
787 needs to be reworked or maintained to account for this. For example, a physical object at  
788 time  $t+1$  will likely be different than at time  $t$ . However, the digital twin should be the  
789 same at times  $t$  and  $t+1$  unless it updates dynamically with feeds from the physical object.  
790 Having access to an accurate timestamp [26] for the physical object and digital twin is a  
791 trust consideration.
- 792 3. **Environment:** The digital twin paradigm has an implied or explicit environmental  
793 component that cannot be overlooked. For physical objects, a description of the  
794 environmental tolerances or expected usage profiles is needed for many of the “ilities”  
795 [27], particularly interoperability. For example, bricks used to construct buildings are  
796 made from a variety of materials; some bricks will break easier under stress than others  
797 and some bricks are better suited to certain temperatures and climates. This additional  
798 expected operational usage information should be stored with a digital twin. Without this,  
799 it will be difficult to determine if the physical object is “fit for purpose” since purpose

- 800 implies environment and context. Unknown environmental influences have plagued  
801 safety-critical systems and software. Consider PowerPoint running during a presentation.  
802 Usually, the presenter does little more than touch the Page-Up or Page-Down keys. One  
803 could argue that the operational profile for executing PowerPoint during a presentation is  
804 two-fold: 1) the loaded presentation and 2) the button inputs from the presenter.  
805 However, whether the presentation goes smoothly (e.g., reliably and in a timely manner)  
806 is also a function of all of the inputs that PowerPoint is receiving from the disk, memory,  
807 and the OS in real time. If, for example, the presentation gets stuck going from slide x to  
808 slide x+1 then something related to “unknown” (phantom-like) environmental influences  
809 is probably involved (e.g., another process running on the machine at the same time and  
810 stealing resources and computing cycles). Accurately defining as many environmental  
811 factors as possible is a trust consideration.
- 812 4. **Manufacturing Defects:** The digital twin paradigm has an interesting relationship to  
813 mass production. A digital twin may be used to guide a manufacturing process. For  
814 example, a factory that produces light bulbs will have a certain defect rate per thousand  
815 bulbs. Not all bulbs produced will be usable, and for those that are usable there will still  
816 be small (possibly microscopic) distinctions between individual bulbs. These small  
817 distinctions may impact the lifetime of a specific bulb. The packaging on a set of light  
818 bulbs will offer an approximation for how long a bulb will operate before burnout. This  
819 highlights that a digital twin could not only describe the underlying components of an  
820 average bulb but also suggest how it should be manufactured if the representation also  
821 details a metric, such as time-to-burnout. Ensuring that a manufacturing process produces  
822 a product with the correct life expectancy based on the information in a digital twin is a  
823 trust consideration.
- 824 5. **Functional Equivalence:** The digital twin paradigm needs a means to determine  
825 functional equivalence between the digital twin and the physical object. Without this,  
826 trust is suspect. If the digital twin is an executable specification, then for the inputs that it  
827 is fed, it should produce the same outputs that the physical object produces for the same  
828 input data. If this does not occur, then functional equivalence has not been achieved. This  
829 could occur for a variety of factors, such as decay and fatigue, manufacturing variances,  
830 or other environmental influences that the physical object experiences during operation  
831 but that the digital twin does not. Without some assessment of the level of functional  
832 equivalence, it is difficult to argue for trustworthiness.
- 833 6. **Composability and Complexity:** There is a trust consideration regarding the size and  
834 complexity of the digital twin for its physical object. A digital twin that is too  
835 complicated can create a composability problem in terms of predicting the  
836 trustworthiness of a final composed system from more than one digital twin. Assume that  
837 a system has five physical components, and each component has a digital twin.  
838 Physically connecting the five components may be straightforward but composing the  
839 five digital twins may not be, particularly if the digital twins contain information such as  
840 tolerances and expected operational usages. Standards should be useful to prune  
841 extraneous information contained in a digital twin since standards can define required  
842 interconnects between components of a domain enabling the composition to be modelled  
843 and tested. One approach might be separating classes of information into categories, such

844 as “need to know” or “extraneous.”

- 845 7. **Instrumentation and Monitoring:** Instrumentation of a digital twin is a beneficial and  
846 unique advantage that digital twins offer. While one might not be able to instrument the  
847 physical object, one may be able to instrument the digital twin. However, instrumentation  
848 and probes are not as simple or easy to correctly inject into a digital twin as might be  
849 expected; much can be learned here from the safety-critical software community. First, a  
850 determination of where to inject the probes is necessary [28]; this is not often easy and  
851 can be more art than science. Second, how many probes to inject is also a consideration.  
852 As shown in real-time systems, probes can slow down performance and timing. This may  
853 cause a problem for synchronization between the digital twin and physical object. That  
854 said, there are ways to reduce this impact by having the probes only collecting raw data  
855 and not compute internal test results, such as built-in self-tests. Collecting the “right”  
856 information from the internal state of an executing digital twin is an expensive and error-  
857 prone effort.
- 858 8. **Heterogeneity of Standards:** Heterogeneity of different formats for digital twins may  
859 cause composability problems [29]. If vendors misuse standardized formats for the digital  
860 twins of their components, composing digital twins from different component vendors  
861 may not be achievable [4]. This is a consideration for trusting composed digital twins.
- 862 9. **Non-functional Requirements:** A trust consideration for systems composed of many  
863 components deals with quality attributes often referred to as “ilities.” This also applies to  
864 digital twin technology. Functional requirements state what a system shall do; negative  
865 requirements state what a system shall not do; and non-functional requirements (i.e., the  
866 “ilities”) typically state what level of quality the system shall exhibit both for the  
867 functional and negative requirements. “ilities” apply to both “things” and the systems  
868 they are built into. It is unclear how many “ilities” there are, though examples include  
869 availability, composability, compatibility, dependability, discoverability, durability, fault  
870 tolerance, flexibility, interoperability, insurability, liability, maintainability, observability,  
871 privacy, performance, portability, predictability, probability of failure, readability,  
872 reliability, resilience, reachability, safety, scalability, cybersecurity, sustainability,  
873 testability, traceability, usability, visibility, and vulnerability [27]. The issue for digital  
874 twin technology concerns how many of the non-functional requirements can be written  
875 for the functional and negative requirements (thus defining the level of quality for what  
876 the system should and should not do). The ability to write these non-functional  
877 requirements will affect the ability to claim the trustworthiness of a composite object.
- 878 10. **Digital Twin Accuracy:** If the accuracy of a digital twin is questionable, or even found  
879 to be faulty, then trust is an issue. For software, faulty specifications lead to faulty  
880 designs that lead to faulty implementations. In digital twin technology, the degree to  
881 which the digital twin is correct is a trust consideration. It begs the question as to whether  
882 it might be prudent to have more than one independently created digital twin for a  
883 specific physical object. In n-version programming [30], more than one independent  
884 software implementation is created for highly critical systems that the software impacts  
885 because no single implementation can be assumed to be adequately trustworthy. To  
886 address this, each independent implementation is run in parallel, and the outputs from

- 887 each implementation are sent to a voter that then decides on the final output that the  
888 system receives.
- 889 11. **Testing:** The testability of digital twins refers to measuring how likely an error or defect  
890 will be detected during testing. Systems that are less likely to reveal the presence of  
891 defects are deemed less testable. Physical objects are testable to different degrees using  
892 this definition, though the methods for testing digital twins that are most likely to  
893 demonstrate that the digital representation is correct are unclear. One option is to ignore  
894 this trust consideration and decide that a digital twin is untestable and, therefore, stands  
895 alone as the “oracle” or “gold standard.” Moreover, although testing usually involves  
896 expected use cases, consideration should also be given for cases of misuse.
- 897 12. **Certification:** Certification usually occurs in two different ways [31]. One type certifies  
898 the process used to develop, while the other certifies the final artifact that comes from  
899 that process. These two types of certification are distinct [3][32][33][34][35][36][37]. For  
900 digital twin technology, this means that one could attempt to certify how the digital twin  
901 was created or certify the accuracy of the digital twin itself. Certification of a twin will be  
902 complicated. For example, the pharmaceutical industry has illuminated the problem of  
903 information overload. Most prescription drugs come with warnings concerning who can  
904 take them based on sex, age, underlying conditions, negative drug interactions, and other  
905 factors. Most drugs come with disclaimers about negative side effects and when to  
906 discontinue use. This information is made available to patients, doctors, pharmacists, and  
907 other medical providers. The problem stems from the vast amount of information known  
908 about a drug and the vaster amount of unknown information about a drug at time  $t$  that  
909 will not be known until time  $t+1$ . Further, much of the information is only understandable  
910 by medical experts but is vital to determine a drug’s fitness for purpose. The trust  
911 consideration here for digital twin technology is how much of this information can be  
912 provided in a digital twin description without overloading a twin with extraneous  
913 information that leads to confusion about how to use the twin or what the twin even  
914 represents.
- 915 13. **Propagation:** One of the greatest trust concerns with any *system of systems* is how errors  
916 and corrupt data propagate (cascade) during execution [38][39]. The digital twin  
917 paradigm experiences this trust consideration, particularly when different twins  
918 representing different physical objects are composed. This may, perhaps, suggest that  
919 twins should be wrapped with pre-conditions and post-conditions to determine if the  
920 output from one twin will be acceptable as input to another twin.
- 921 14. **Counterfeiting:** It is possible that a digital twin could be tampered with or counterfeited.  
922 There are schemes that could be used to protect against this. Digital twins could be  
923 hashed, and the hash posted to a public web page; users of a digital twin could hash their  
924 copy and compare it against the hash on the public web page. This said, web pages and  
925 other similar publicly accessible repositories can be hacked. To enhance trust here one  
926 could use a blockchain and post a digital twin hash publicly in an immutable data  
927 structure (it could never be changed even by malicious attackers). In these ways  
928 modifications to digital twin files could be discovered. Alternatively, identical copies of a  
929 digital twin could be stored in separate locations (e.g., in offline backups).

930

**931 9 Conclusions**

932 Digital twin is an emerging area of research and standardization. At the same time its core  
933 elements of modeling and simulation are already very mature and widely used. Other significant  
934 components, such as virtual reality, are also frequently deployed (even as low-cost gaming units  
935 in homes) and IoT sensors are becoming commonplace. Because of this, there may be a lack of  
936 clarity as to what is new with digital twins and what promise this technology holds. In this work  
937 we attempted to provide this clarity. We provided a detailed definition of digital twins, the  
938 motivation and vision for their use, common low-level operations, usage scenarios, and example  
939 use cases.

940 We also focused on technical considerations with the cybersecurity and trust of digital twins. We  
941 analyzed novel cybersecurity challenges arising from the use of digital twin architectures and  
942 then looked at the traditional cybersecurity challenges that apply. We evaluated trust issues and  
943 what a lack of trust and standards can do to digital twin functionality and quality. And we  
944 mapped our evaluations where appropriate to other NIST cybersecurity guidance.

945 It is our hope that our documentation of a definition and vision for digital twins along with an  
946 evaluation of cybersecurity and trust considerations will be useful in progressing this technology.  
947 In particular, we hope that standards developers and digital twin implementers will use this  
948 document to ensure the secure and trustworthy development of digital twin standards and  
949 architectures.

950 **References**

- 951 [1] The Definition of a Digital Twin. [https://www.digitaltwinconsortium.org/hot-topics/the-](https://www.digitaltwinconsortium.org/hot-topics/the-definition-of-a-digital-twin.htm)  
952 [definition-of-a-digital-twin.htm](https://www.digitaltwinconsortium.org/hot-topics/the-definition-of-a-digital-twin.htm). (accessed 2021).
- 953 [2] Merriam-Webster online dictionary of American English. <http://www.m-w.com> (accessed  
954 2021).
- 955 [3] Jeffrey M. Voas, George Hurlburt. “Third Party Software’s Trust Quagmire.” IEEE  
956 Computer, Volume 48 Issue 12:80-87.
- 957 [4] Jeffrey M. Voas, Phillip A. Laplante. July 2007. “Standards Confusion and Harmonization.”  
958 IEEE Computer Volume 40 Issue 7: 94-96.
- 959 [5] Piroumian, Vartan. January 2021. “Digital Twins: Universal Interoperability for the Digital  
960 Age.” IEEE Computer Volume 54, Number 1: 61-69.
- 961 [6] HTML 5.2, W3C Recommendation, 17 December 2017, superseded 28 January 2021.  
962 <https://www.w3.org/TR/html52/> (accessed 2021).
- 963 [7] HTML Element Reference. W3schools.com <https://www.w3schools.com/tags/default.asp> .  
964 (accessed 2021).
- 965 [8] 3D PDF Consortium. “PDF in Manufacturing.” 2020. pp 22-26.
- 966 [9] Adele Goldberg. Smalltalk-80: The Interactive Programming Environment. Reading, MA.  
967 Addison-Wesley. 1983.
- 968 [10] Edward Yourdon, Larry Constantine. Structured Design: Fundamentals of a Discipline of  
969 Computer Program and Systems Design. Upper Saddle River, NJ. Prentice-Hall. 1979.
- 970 [11] G. Booch, Object-Oriented Analysis and Design with Applications. Redwood City, CA:  
971 Benjamin/Cummings. 1990.
- 972 [12] Robert L. Woods, Kent L. Lawrence. Modeling and Simulation of Dynamic Systems.  
973 Englewood Cliffs, NJ. Prentice Hall. 1997.
- 974 [13] “Internet Streaming: What It Is and How It Works.” 2021.  
975 <https://www.lifewire.com/internet-streaming-how-it-works-1999513> (accessed 2021).
- 976 [14] “What Is Streaming? How Video Streaming Works.” Sam Costello. (accessed 2021).  
977 <https://www.cloudflare.com/learning/video/what-is-streaming/>
- 978 [15] John C. Reynolds. Theories of Programming Languages. Cambridge. Cambridge  
979 University Press. 1998.
- 980 [16] Robert Scheifler, James Gettys, Jim Flowers, David Rosenthal. X Window System, The

- 981 Complete Reference to Xlib, X Protocol, ICCCM, XLFD. Digital Press. 1992.
- 982 [17] Catuscia Palamidessi, Hugh Glaser, Karl Meinke. Principles of Declarative Programming:  
983 10th Annual Symposium PLILP'98. Springer. 1998.
- 984 [18] Roberto Minerva, Gyu Myoung Lee, Noël Crespi. Digital Twin in the IoT Context: A  
985 Survey on Technical Features, Scenarios, and Architectural Models. Proceedings of the IEEE  
986 Volume 108, Number 10. October 2020.
- 987 [19] Digital Twin Consortium. [https:// www.digitaltwinconsortium.org](https://www.digitaltwinconsortium.org) (accessed 2020).
- 988 [20] NIST Risk Management Framework. <https://csrc.nist.gov/projects/risk-management>  
989 (accessed 2021).
- 990 [21] NIST Cybersecurity Framework. <https://www.nist.gov/cyberframework> (accessed 2021).
- 991 [22] NIST Privacy Framework. <https://www.nist.gov/privacy-framework> (accessed 2021).
- 992 [23] NIST, “Security and Privacy Controls for Information Systems and Organizations”. 2020.  
993 <https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final> (accessed 2021).
- 994 [24] NIST Cybersecurity for IoT Program. [https://www.nist.gov/programs-projects/nist-](https://www.nist.gov/programs-projects/nist-cybersecurity-iot-program)  
995 [cybersecurity-iot-program](https://www.nist.gov/programs-projects/nist-cybersecurity-iot-program) (accessed 2021).
- 996 [25] Alper Kerman, Oliver Borchert, Scott Rose, Eileen Division, Allen Tan, “Implementing a  
997 Zero Trust Architecture” [https://www.nccoe.nist.gov/library/implementing-zero-trust-](https://www.nccoe.nist.gov/library/implementing-zero-trust-architecture)  
998 [architecture](https://www.nccoe.nist.gov/library/implementing-zero-trust-architecture) (accessed 2021).
- 999 [26] A. Stavrou & J. Voas, “Verified time,” IEEE Computer, Vol. 50, 2017.
- 1000 [27] J. Voas, “Software’s secret sauce: The ‘ilities’,” Quality Time Column, IEEE Software,  
1001 21(6), pp. 2-3, November 2004.
- 1002 [28] J. Voas & K. Miller. “Putting Assertions in Their Place,” Proceedings of the International  
1003 Symposium on Software Reliability Engineering, November 1994, Monterey, CA
- 1004 [29] J. Voas, Networks of Things, NIST Special Publication (SP) 800-183, National Institute of  
1005 Standards and Technology, Gaithersburg, Maryland, 2016.
- 1006 [30] N-Version Programming: A Fault-Tolerance Approach to Reliability of Software Operation,  
1007 Liming Chen; Avizienis, A., Fault-Tolerant Computing, 1995, ' Highlights from Twenty-Five  
1008 Years'. , Twenty-Fifth International Symposium on, Vol., Iss., 27-30 Jun 1995.
- 1009 [31] J. Voas, “The Software Quality Certification Triangle,” Crosstalk, 11(11), pp. 12-14,  
1010 November 1998.
- 1011 [32] J. Voas, “Certifying off-the-shelf software components,” IEEE Computer, 31(6): 53-59,

- 1012 June 1998.
- 1013 [33] J. Voas, "Certifying software for high assurance environments," IEEE Software, 16(4), pp.  
1014 48-54, July 1999.
- 1015 [34] J. Voas & J. Payne, "Dependability certification of software components," Journal of  
1016 Systems and Software, Vol. 52, p. 165-172, 2000.
- 1017 [235] J. Voas, "Toward a Usage-Based Software Certification Process," IEEE Computer, 33(8),  
1018 pp. 32-37, August 2000.
- 1019 [36] J. Voas & P. Laplante, "The IoT Blame Game," IEEE Computer, 2017.
- 1020 [37] J. Voas & P. Laplante, "IoT's certification quagmire," IEEE Computer, April 2018.
- 1021 [38] J. Voas, "Error propagation analysis for COTS systems," IEEE Computing and Control  
1022 Engineering Journal, 8(6), pp. 269-272, December 1997.
- 1023 [39] J. Voas, F. Charron, & K. Miller, "Tolerant Software Interfaces: Can COTS-based systems  
1024 be trusted without them?" Proceedings of the 15<sup>th</sup> International Conference on Computer Safety,  
1025 Reliability and Security (SAFECOMP'96), Springer-Verlag, pp. 126-135, October 1996.

1026 **Appendix A—Glossary**

1027

**digital twin**

The digital representation of a real-world entity, concept, or notion, either physical or perceived.

1028

**1029 Appendix B—Acronyms**

1030 Selected acronyms and abbreviations used in this paper are defined below.

1031	2D	Two dimensional
1032	3D	Three dimensional
1033	AI	Artificial Intelligence
1034	AR	Augmented Reality
1035	A/V	Audio/Visual
1036	CNC	Computer Numerical Control
1037	COTS	Commercial Off-the-Shelf
1038	DT	Digital Twin
1039	GUI	Graphical User Interface
1040	HTML	HyperText Markup Language
1041	IC	Integrated Circuit
1042	IoT	Internet of Things
1043	IT	Information Technology
1044	MVC	Model-view-controller
1045	NIST	National Institute of Standards and Technology
1046	PCB	Printed Circuit Board
1047	PDF	Portable Document Format
1048	SDO	Standards Developing Organization
1049	UAV	Unmanned Aerial Vehicle
1050	UI	User Interface
1051	VR	Virtual Reality
1052	WYSIWYG	What-you-see-is-what-you-get

1053	WiFi	Wireless Fidelity <sup>1</sup>
1054	XML	eXtensible Markup Language

---

<sup>1</sup> A family of wireless network protocols.