IEEE SA
STANDARDS ASSOCIATION

IEEE/UL Recommended Practice for Wireless Diabetes Device Security: Use of Mobile Devices in Diabetes Control Contexts

STANDARDS

IEEE Engineering in Medicine and Biology Society

Developed by the
IEEE Engineering in Medicine and
Biology Standards Committee

IEEE Std 2621.3™-2022/UL 2621-3:2022

IEEE

IEEE/UL Recommended Practice for Wireless Diabetes Device Security: Use of Mobile Devices in Diabetes Control Contexts

Developed by the

IEEE Engineering in Medicine and Biology Standards Committee
of the
IEEE Engineering in Medicine and Biology Society

Approved 24 March 2022

IEEE SA Standards Board

Recognized as an American National Standard

Abstract: A framework for a connected electronic product security evaluation program, with specific requirements and guidance relating to digital diabetes devices and solutions, such as insulin pumps is defined in this standard.

Keywords: assurance, devices, diabetes, evaluator, firmware, IEEE 2621.3™, protection profile, security, security target

The Institute of Electrical and Electronics Engineers, Inc.
3 Park Avenue, New York, NY 10016-5997, USA

ULSE Inc.
333 Pfingsten Road
Northbrook, IL 60062

PDF: ISBN 978-1-5044-8584-5 STD25340
Print: ISBN 978-1-5044-8585-2 STDPD25340

Commitments for amendments

This Standard is issued jointly by the Institute of Electrical and Electronics Engineers, Inc. (IEEE) and ULSE Inc. (ULSE) Comments or proposals for revisions or any part of the standard may be submitted to IEEE and/or ULSE at any time. Revisions to this Standard will be made only after processing according to the Standards development procedures of IEEE and ULSE.

Comments or proposals for revisions on any part of the Standard may be submitted to ULSE Inc. at any time. Proposals should be submitted via a Proposal Request in ULSE's On-Line Collaborative Standards Development System (CSDS) at https://csds.ul.com.

Any person who would like to participate in evaluating comments or in revisions to an IEEE standard is welcome to join the relevant IEEE working group. You can indicate interest in a working group using the Interests tab in the Manage Profile & Interests area of the IEEE SA myProject system.[1] An IEEE Account is needed to access the application.

Comments on IEEE standards should be submitted using the Contact Us form.[2]

Copyrights

IEEE draft and approved standards are copyrighted by IEEE under US and international copyright laws. They are made available by IEEE and are adopted for a wide variety of both public and private uses. These include both use, by reference, in laws and regulations, and use in private self-regulation, standardization, and the promotion of engineering practices and methods. By making these documents available for use and adoption by public authorities and private users, IEEE does not waive any rights in copyright to the documents.

UL's Standards for Safety are copyrighted by ULSE Inc. Neither a printed nor electronic copy of a Standard should be altered in any way. All of UL's Standards and all copyrights, ownerships, and rights regarding those Standards shall remain the sole and exclusive property of ULSE Inc.

To purchase UL Standards, visit ULSE's Standards Sales site at:

http://www.shopulstandards.com/HowToOrder.aspx or call toll-free 1-888-853-3503.

Important Notices and Disclaimers Concerning IEEE Standards Documents

IEEE Standards documents are made available for use subject to important notices and legal disclaimers. These notices and disclaimers, or a reference to this page (https://standards.ieee.org/ipr/disclaimers.html), appear in all standards and may be found under the heading "Important Notices and Disclaimers Concerning IEEE Standards Documents."

Notice and Disclaimer of Liability Concerning the Use of IEEE Standards Documents

IEEE Standards documents are developed within the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (IEEE SA) Standards Board. IEEE develops its standards through an accredited consensus development process, which brings together volunteers representing varied

[1]Available at: https://development.standards.ieee.org/myproject-web/public/view.html#landing.
[2]Available at: https://standards.ieee.org/content/ieee-standards/en/about/contact/index.html.

viewpoints and interests to achieve the final product. IEEE Standards are documents developed by volunteers with scientific, academic, and industry-based expertise in technical working groups. Volunteers are not necessarily members of IEEE or IEEE SA, and participate without compensation from IEEE. While IEEE administers the process and establishes rules to promote fairness in the consensus development process, IEEE does not independently evaluate, test, or verify the accuracy of any of the information or the soundness of any judgments contained in its standards.

IEEE makes no warranties or representations concerning its standards, and expressly disclaims all warranties, express or implied, concerning this standard, including but not limited to the warranties of merchantability, fitness for a particular purpose and non-infringement. In addition, IEEE does not warrant or represent that the use of the material contained in its standards is free from patent infringement. IEEE standards documents are supplied "AS IS" and "WITH ALL FAULTS."

Use of an IEEE standard is wholly voluntary. The existence of an IEEE Standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the IEEE standard. Furthermore, the viewpoint expressed at the time a standard is approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standard.

In publishing and making its standards available, IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity, nor is IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing any IEEE Standards document, should rely upon his or her own independent judgment in the exercise of reasonable care in any given circumstances or, as appropriate, seek the advice of a competent professional in determining the appropriateness of a given IEEE standard.

IN NO EVENT SHALL IEEE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO: THE NEED TO PROCURE SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE PUBLICATION, USE OF, OR RELIANCE UPON ANY STANDARD, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE AND REGARDLESS OF WHETHER SUCH DAMAGE WAS FORESEEABLE.

Translations

The IEEE consensus development process involves the review of documents in English only. In the event that an IEEE standard is translated, only the English version published by IEEE is the approved IEEE standard.

Official statements

A statement, written or oral, that is not processed in accordance with the IEEE SA Standards Board Operations Manual shall not be considered or inferred to be the official position of IEEE or any of its committees and shall not be considered to be, nor be relied upon as, a formal position of IEEE. At lectures, symposia, seminars, or educational courses, an individual presenting information on IEEE standards shall make it clear that the presenter's views should be considered the personal views of that individual rather than the formal position of IEEE, IEEE SA, the Standards Committee, or the Working Group.

Comments on standards

Comments for revision of IEEE Standards documents are welcome from any interested party, regardless of membership affiliation with IEEE or IEEE SA. However, **IEEE does not provide interpretations, consulting information, or advice pertaining to IEEE Standards documents**.

Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Since IEEE standards represent a consensus of concerned interests, it is important that any responses to comments and questions also receive the concurrence of a balance of interests. For this reason, IEEE and the members of its Societies and Standards Coordinating Committees are not able to provide an instant response to comments, or questions except in those cases where the matter has previously been addressed. For the same reason, IEEE does not respond to interpretation requests. Laws and regulations

Users of IEEE Standards documents should consult all applicable laws and regulations. Compliance with the provisions of any IEEE Standards document does not constitute compliance to any applicable regulatory requirements. Implementers of the standard are responsible for observing or referring to the applicable regulatory requirements. IEEE does not, by the publication of its standards, intend to urge action that is not in compliance with applicable laws, and these documents may not be construed as doing so.

Data privacy

Users of IEEE Standards documents should evaluate the standards for considerations of data privacy and data ownership in the context of assessing and using the standards in compliance with applicable laws and regulations.

Photocopies

Subject to payment of the appropriate licensing fees, IEEE will grant users a limited, non-exclusive license to photocopy portions of any individual standard for company or organizational internal use or individual, non-commercial use only. To arrange for payment of licensing fees, please contact Copyright Clearance Center, Customer Service, 222 Rosewood Drive, Danvers, MA 01923 USA; +1 978 750 8400; https://www.copyright.com/. Permission to photocopy portions of any individual standard for educational classroom use can also be obtained through the Copyright Clearance Center.

Updating of IEEE Standards documents

Users of IEEE Standards documents should be aware that these documents may be superseded at any time by the issuance of new editions or may be amended from time to time through the issuance of amendments, corrigenda, or errata. An official IEEE document at any point in time consists of the current edition of the document together with any amendments, corrigenda, or errata then in effect.

Every IEEE standard is subjected to review at least every 10 years. When a document is more than 10 years old and has not undergone a revision process, it is reasonable to conclude that its contents, although still of some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that they have the latest edition of any IEEE standard.

In order to determine whether a given document is the current edition and whether it has been amended through the issuance of amendments, corrigenda, or errata, visit IEEE Xplore or contact IEEE.[3] For more information about the IEEE SA or IEEE's standards development process, visit the IEEE SA Website.

[3]Available at: https://ieeexplore.ieee.org/browse/standards/collection/ieee.

Errata

Errata, if any, for all IEEE standards can be accessed on the IEEE SA Website.[4] Search for standard number and year of approval to access the web page of the published standard. Errata links are located under the Additional Resources Details section. Errata are also available in IEEE Xplore. Users are encouraged to periodically check for errata.

Patents

IEEE Standards are developed in compliance with the IEEE SA Patent Policy.[5]

Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken by the IEEE with respect to the existence or validity of any patent rights in connection therewith. If a patent holder or patent applicant has filed a statement of assurance via an Accepted Letter of Assurance, then the statement is listed on the IEEE SA Website at https://standards.ieee.org/about/sasb/patcom/patents.html. Letters of Assurance may indicate whether the Submitter is willing or unwilling to grant licenses under patent rights without compensation or under reasonable rates, with reasonable terms and conditions that are demonstrably free of any unfair discrimination to applicants desiring to obtain such licenses.

Essential Patent Claims may exist for which a Letter of Assurance has not been received. The IEEE is not responsible for identifying Essential Patent Claims for which a license may be required, for conducting inquiries into the legal validity or scope of Patents Claims, or determining whether any licensing terms or conditions provided in connection with submission of a Letter of Assurance, if any, or in any licensing agreements are reasonable or non-discriminatory. Users of this standard are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. Further information may be obtained from the IEEE Standards Association.

IMPORTANT NOTICE

IEEE Standards do not guarantee or ensure safety, security, health, or environmental protection, or ensure against interference with or from other devices or networks. IEEE Standards development activities consider research and information presented to the standards development group in developing any safety recommendations. Other information about safety practices, changes in technology or technology implementation, or impact by peripheral systems also may be pertinent to safety considerations during implementation of the standard. Implementers and users of IEEE Standards documents are responsible for determining and complying with all appropriate safety, security, environmental, health, and interference protection practices and all applicable laws and regulations.

[4]Available at: https://standards.ieee.org/standard/index.html.
[5]Available at: https://standards.ieee.org/about/sasb/patcom/materials.html.

Participants

At the time this IEEE standard was completed, the Healthcare Device Security Assurance Working Group had the following membership:

David Klonoff, *Chair*
David Kleidermacher, *Co-Chair*

Aiman Abdel-Malek	Barry Ginsberg	Patricia Sena
Carole C. Carey	Julia Han	Trisha Shang
Kong Chen	Diana Pappas Jordan	Christine Sublett
Sean Donahue	Christopher Keegan	Nicole Y. Xu
Anura Fernando	Kevin T. Nguyen	Jennifer Y. Zhang
Brian Fitzgerald	Naomi Schwartz	Margie Zuk

The following members of the individual Standards Association balloting group voted on this standard. Balloters may have voted for approval, disapproval, or abstention.

Pradeep Balachandran	Werner Hoelzl	Ting Li
Brian Blum	Piotr Karocki	Rajesh Murthy
Carole C. Carey	Edmund Kienast	Esteban Pino
Diego Chiozzi	David Kleidermacher	Naomi Schwartz
Todd Cooper	David Klonoff	Walter Struppler

When the IEEE SA Standards Board approved this standard on 24 March 2022, it had the following membership:

David J. Law, *Chair*
Ted Burse, *Vice Chair*
Gary Hoffman, *Past Chair*
Konstantinos Karachalios, *Secretary*

Edward A. Addy	Johnny Daozhuang Lin	Mark Siira
Ramy Ahmed Fathy	Kevin Lu	Dorothy V. Stanley
J.Travis Griffith	Daleep C. Mohla	Lei Wang
Guido R. Hiertz	Andrew Myles	F.Keith Waters
Yousef Kimiagar	Damir Novosel	Karl Weber
Joseph L. Koepfinger*	Annette D. Reilly	Sha Wei
Thomas Koshy	Robby Robson	Philip B. Winston
John D. Kulick	Jon Walter Rosdahl	Daidi Zhong

*Member Emeritus

Introduction

This introduction is not part of IEEE Std 2621.3-2022/UL 2621-3:2022 IEEE/UL Recommended Practice for Wireless Diabetes Device Security: Guidance for Mobile Devices.

The need for medical device functionality and safety has become more challenging with the growing use of wireless and Internet-connected devices. For example, can operation of the device be impacted by loss of wireless connectivity due to interference or malicious jamming? Indeed, an important component of safety is security: malicious attacks against these devices (e.g., via their network connections) should not adversely impact functionality and safety.

In addition, there is significant increased use of off-the-shelf consumer mobile devices (CMDs), (e.g., smartphones) in medical contexts. While these contexts have historically been limited to monitoring rather than control of the medical device and its safety functions, there is increasing patient demand for the use of such mobile devices for control applications. For example, the use of a smartphone app can replace a custom insulin pump remote controller, reducing time-to-market and cost of new treatments while providing for an improved user experience and quality of life for people with diabetes.

In order to realize the potential beneficial uses of consumer digital technology, the medical community, including device manufacturers, regulators, caregivers, and patients should be aware of the risks associated with the use of CMDs and apps in these contexts and follow appropriate regulatory, developmental, lifecycle management, and usage guidelines so that proper functionality and can be maintained.

This standard was developed following research and consultation with a multi-stakeholder community consisting of the US FDA, independent cybersecurity experts, consumer technology developers (e.g., smartphone developers, smartphone operating system developers, and smartphone chipset developers), diabetes device developers, medical research funding agencies, physicians, educators, consumers, regulatory experts, liability attorneys, policy experts, and more. This standard has been developed to identify issues and best practices relating to CMD use in medical contacts. The same stakeholder groups and other applicable interested parties should consider this standard in the design, development, evaluation, approval, management, deployment, and use of CMDs in medical control contexts.

The recommendations contained in this standard are intended to supplement existing standards and guidance, including (in the United States, for example) FDA recognized standards such as ISO/IEC 62304 [B4] and FDA guidance such as the Content of Premarket Submissions for Management of Cybersecurity in Medical Devices [B5].[6] These guidelines describe current consensus thinking of the aforementioned multi-stakeholder community membership on this topic and should be viewed only as recommendations, unless mandatory requirements are states, or specific regulatory or statutory requirements are cited.

Multi-part Standard

This standard is a multi-part standard consisting of the following parts:

— IEEE Std 2621.1™/UL 2621-1-2022 (connected electronic product security evaluation programs)

— IEEE Std 2621.2™/UL 2621-2:2022 (information security requirements for connected diabetes solutions)

— IEEE Std 2621.3™/UL 2621-3:2022 [use of mobile devices in diabetes control contexts (this part)]

[6]The numbers in brackets correspond to those of the bibliography in Annex B.

Contents

IEEE/UL Recommended Practice for Wireless Diabetes Device Security: Use of Mobile Devices in Diabetes Control Contexts

1. Overview

1.1 Scope

This recommended practice specifies recommendations for the use of consumer mobile devices (CMDs) in the control of diabetes-related medical devices. While these recommendations may be applied to other medical use cases, they are targeted specifically for diabetes related control use cases. The following two use cases are covered by this recommended practice: open loop remote control and automated insulin dosing (AID) systems. In general, the recommendations within this recommended practice apply to both use cases unless explicitly indicated otherwise.

1.1.1 Open loop use case

One or more mobile applications (apps) running on a CMD are used to perform some command operation, upon request by the CMD user, on a wirelessly connected diabetes device. For example, a diabetes control app may provide a user interface that enables the user to specify the amount of insulin to be dosed by a wirelessly connected insulin pump. The CMD and its diabetes-related apps replace the traditional remote-control medical device manufactured by a medical device supplier.

1.1.2 Automated insulin dosing (AIM) control use case

The CMD is used to host software that performs some portion of a AID control system. For example, a continuous glucose monitoring system transmits (via wireless network) sensor readings to a CMD app; the CMD app executes an algorithm to compute treatments of insulin; the CMD autonomously transmits (via wireless network) treatment commands to an insulin pump. The CMD and its diabetes-related apps are executing a continuously repeating algorithm for which each algorithm computation results in a treatment to the patient that should be delivered within some developer-specified time frame in order to maintain use.

1.1.3 Explicitly not in scope

This document does not cover standards or guidance already covered in other, pre-existing medical standards and guidance. For example, for the remote-control use case, this guidance does not explain how a developer of a remote-control solution, which happens to use a CMD and CMD software, follows existing FDA-recommended development standards or other regulatory body standards and obtains regulatory approvals to

develop and deploy that remote-control solution. Rather, this guidance discusses the additional considerations related to the use of CMDs in the context of existing standards and approvals.

1.2 Purpose

This recommended practice defines recommendations for the use of mobile devices in diabetes contexts, as deemed necessary and sufficient by an appropriate set of stakeholders. These recommendations are intended to be used within a security evaluation program, as defined in other components of this multi-part standard.

1.3 Word usage

The word *shall* indicates mandatory requirements strictly to be followed in order to conform to the standard and from which no deviation is permitted (*shall* equals is *required to*).[7,8]

The word *should* indicates that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others; or that a certain course of action is preferred but not necessarily required (*should* equals is *recommended that*).

The word *may* is used to indicate a course of action permissible within the limits of the standard (*may* equals is *permitted to*).

The word *can* is used for statements of possibility and capability, whether material, physical, or causal (*can* equals is *able to*).

2. Normative references

The following referenced documents are indispensable for the application of this document (i.e., they must be understood and used, so each referenced document is cited in text and its relationship to this document is explained). For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments or corrigenda) applies.

IEEE Std 2621.2/UL 2621-2:2022, IEEE Standard for Wireless Diabetes Device Security: Information Security Requirements for Connected Diabetes Solutions.[9,10]

ISO/IEC 18045, Information technology—Security techniques—Methodology for IT security evaluation.[11]

3. Definitions, acronyms, and abbreviations

3.1 Definitions

For the purposes of this document, the following terms and definitions apply. The *IEEE Standards Dictionary Online* should be consulted for terms not defined in this clause. [12]

[7]The use of the word *must* is deprecated and cannot be used when stating mandatory requirements, *must* is used only to describe unavoidable situations.
[8]The use of *will* is deprecated and cannot be used when stating mandatory requirements, *will* is only used in statements of fact.
[9]The IEEE standards or products referred to in this clause are trademarks of The Institute of Electrical and Electronics Engineers, Inc.
[10]IEEE publications are available from The Institute of Electrical and Electronics Engineers, 445 Hoes Lane, Piscataway, NJ 08854, USA (https://standards.ieee.org/).
[11]ISO/IEC publications are available from the ISO Central Secretariat (https://www.iso.org/). ISO/IEC publications are available in the United States from the American National Standards Institute (https://www.ansi.org/).
[12]*IEEE Standards Dictionary Online* is available at: http://dictionary.ieee.org. An IEEE Account is required for access to the dictionary, and one can be created at no charge on the dictionary sign-in page.

administrator: The administrator is responsible for management activities, including setting the policy that is applied by the service provider, on the device. If the security policy is defined during manufacturing and never changed, then the developer acts as administrator. If management activities can be performed by the user, then the user may also act as administrator.

assurance: Grounds for confidence that a Target of Evaluation (TOE) meets its security functional requirements (SFRs).

availability: The capability of a system or component to be in a state to execute the function required under given conditions, at a certain time or in a given period, supposing the required external resources are available.

degradation: The strategy for providing safety by design after the occurrence of failures.

developer: The entity that brings to market a solution to which this standard applies; while the traditional developer in this sense is a medical device manufacturer, the entity may be some other systems integrator or service provider that is responsible for the safe and secure development and market deployment of the solution.

evaluator: An independent testing laboratory that evaluates the Target of Evaluation (TOE) against its security target (ST) by analyzing documentation and performing activities such as vulnerability assessment.

failure: The termination of the ability of an element to perform a function as required.

immutable firmware: Firmware that cannot, by design, be modified through unauthorized means. Examples of immutable firmware include firmware written to read-only memory (ROM) or electrically erasable programmable (EEPROM) whose re-programmability is protected against unauthorized use.

personal area network (PAN): The local wireless network used to connect a consumer mobile device (CMD) to one or more medical devices to create an overall medical solution.

protection profile (PP): The set of standardized security requirements for a product class, such as connected diabetes devices.

real-time: The actual time during which an activity shall take place.

security target (ST): The manifestation or mapping of protection profile (PP) requirements for a specific, individual electronic product, for example a specific version/SKU of a manufacturer's insulin pump. An ST may also cover multiple, similar instances (e.g., a product family with common security requirements).

sufficient resilience: Permitting the remediation of situational risk to the patient.

Target of Evaluation (TOE): A set of software, firmware and/or hardware possibly accompanied by guidance.

Target of Evaluation (TOE) security functionality (ST): A set consisting of all hardware, software, and firmware of the TOE that shall be relied upon for the correct enforcement of the security functional requirements (SFRs).

user: The authorized operator of the Target of Evaluation (TOE). For a diabetes device, the primary owner and patient is the most obvious example of authorized user; however, authorized family members or caregivers assisting the patient are other possible examples of authorized user in this case. An authorized user is assumed to be able to access any of the device's documented user interfaces.

3.2 Acronyms and abbreviations

AID	automated insulin dosing
app	application
CMD	consumer mobile device
MDFPP	Mobile Device Fundamentals Protection Profile
NIAP	National Information Assurance Partnership
PAN	personal area network
PP	protection profile
SFR	security functional requirement
ST	security target

4. Conformance

This clause specifies the mandatory and optional capabilities provided by conformant implementations of this standard. See Annex A for guidance about the use of CMDs that may vary based on the assurance package selected from IEEE Std 2621.2/UL 2621-2.

4.1 Meeting security targets (STs) derived from this standard

Cybersecurity requirements for the medical uses defined in this document's scope are covered by other parts of this multi-part standard. The specific security requirements for a particular solution (e.g., a standalone product or a system composed of multiple products), whether it incorporates the use of a CMD or not, is defined in a security target (ST), according to this standard. Such an ST shall claim conformance to this standard; in particular, the ST shall select one of this standard's defined assurance packages as follows:

— Moderate package, for solutions that require protection against moderate attack potential threats

— Enhanced-basic package, for solutions that require protection against enhanced-basic attack potential threats

— Basic package for solutions that only require vendor affirmation (rather than independent laboratory affirmation) of conformance to this standard's security functional requirements (SFRs)

4.1.1 Additional requirements for security targets (STs) with enhanced-based package

In order to meet enhanced-basic package requirements, evaluators of solutions that leverage CMD apps should require the use of CMDs that either are certified against the most recent version of the National Information Assurance Partnership (NIAP) Mobile Device Fundamentals Protection Profile (MDFPP) or satisfy the following requirements:

— Hardware-rooted verified boot (provides integrity protection, as required by this standard, but evaluators likely may not need to perform rigorous testing)

— Regular security updates (commitment from CMD manufacturer and/or OS developer and previous history of compliance)

— Controls in place to help prevent malware-type behavior (for example, when anti-malware software is embedded within the device or when adopting mechanisms to help prevent the loading of apps from untrusted sources or from unknown developers)

In addition to these device security attributes, the medical software running on the CMD and the medical software running on a connected device as part of the solution should perform additional security checks to verify the medical function is hosted on a CMD that meets the above requirements or at least as many of them as can be attested. Examples of methods for providing this kind of attestation include the following:

— The medical software can only run on known good CMDs (allowlisting via the app store or using mobile device management software).

— The CMD software calls operating system attestation application program interfaces to validate that the software is running on known good CMDs.

— The connected medical device software uses hardware-backed remote attestation to validate that the CMD software is running on known good CMDs (e.g., the device is not rooted or jailbroken).

While good security often assists in privacy, and while data encryption is recommended for privacy-sensitive medical data, privacy-related requirements are not rigorously considered in the scope of this standard. This standard recognizes but does not intend to restate or replace applicable laws and regulations regarding data privacy and security. Users of this standard are responsible for referring to and observing all such laws and regulations. Compliance with the provisions of this standard does not imply compliance with any applicable legal or regulatory requirements.

Ultimately, the ability of a solution to meet the requirements of this standard should be assessed and determined by an authorized independent laboratory within the appropriate evaluation scheme, as defined by other parts of this standard, rather than by developers, users, caregivers, or other stakeholders. Developers and regulators should leverage this multi-part standard when determining the safety suitability of CMDs in medical contexts.

4.1.2 Additional requirements for security targets (STs) with moderate package

At the time of this writing, meeting the moderate package requirements using standard mobile apps on CMDs is challenging due to the existence of a frequent stream of exploitable high severity vulnerabilities in various layers of the operating systems managing these apps. Even with the frequent security patching recommended in 4.1.1, moderate attack potential attackers have been able to locate exploitable so-called “zero day” vulnerabilities given sufficient resources and effort (applicable to the parameters of moderate attack potential per ISO/IEC 18045) dedicated to the task.[13]

Therefore, in order to leverage CMDs for moderate attack potential assurance requirements, the full operating system attack surface area should be avoided, using one of many possible risk reduction techniques. Example techniques may include the following:

— Critical functions may be hosted on a separate security co-processor or other hardware partitioned environment running an independent operating system that is less susceptible to attack due to lower code complexity, lack of attackable surface area (e.g., inability to run arbitrary apps directly on the co-processor), or both.

— The CMD may be locked down using a policy enforcement engine (such as that used by enterprises for corporate liable, fully managed operation) to only allow an allowlisted set of highly trusted apps, limit the methods and peers for wireless connections, and employ potentially other controls, thereby making it more difficult for attackers to leverage mobile operating system vulnerabilities.

— The CMD alone may not be exclusively depended upon for safety and security; for example, a remote control command from the CMD may be double-checked by the user on an insulin pump equipped with its own display.

[13] Information on references can be found in Clause 2.

Increased demand for CMDs in medical contexts may help to encourage CMD manufacturers and other service providers to build and leverage such approaches. Any solution approach taken by a developer should be evaluated by authorized independent testing laboratories for security and compliance as defined in other parts of this standard.

4.1.3 Additional requirements for real-time control and resource availability

In the use of CMDs for medical control, there is a concern about the ability of CMD medical software operations—working alone or in combination with one or more medical devices—to complete reliably and within an expected time-frame, and to obtain access to the required resources to complete their function. For example, when a remote-control operation is initiated by the user, does the remote-control app running on a CMD (relative to a traditional purpose-built remote controller) successfully transmit the control information wirelessly to the controlled medical device within a human-discernible timeframe? In AID control, is a CMD-hosted control algorithm that needs to execute at some fixed periodic interval able to do so without fail (obtaining adequate central processing unit time), as well as having access to other required resources such as memory, communication, etc.? The ability of a system to complete a required task within some specified deadline is sometimes referred to as real-time, although the computing world often disagrees on the precise meaning of this term. Note that in order to complete a task, access to finite resources other than computing time is also required.

The importance of real-time reliability varies on the app, the ramifications of a missed deadline, and the resilience of the system/function to missed deadlines. For example, if the remote-control operation fails to be transmitted to an insulin pump in response to the user's direction (failure of timely access to communication, e.g., radio), the operation may still be safely completed by retrying the transmission or by falling back to manual input on the pump itself. Similarly, an AID algorithm that fails to execute within its developer-specified real-time window may cause an alarm on the insulin pump (driven by the pump itself) that alerts the user to fall back to manual treatment via the insulin pump. Similar arguments can be made for other forms of failure, such as loss of battery power or loss of wireless connectivity, which may prevent the CMD from completing its operation.

The ability of a medical device to meet its safety requirements is covered by existing medical device manufacturing and regulatory approval processes. For example, a remote controller or dedicated AID controller may also lose battery power or connectivity for a variety of reasons, and developers already take such hazards into account in making their safety cases for approval. Therefore, this section covers only additional concerns specific to the use of CMDs in these contexts.

CMDs do not run traditional real-time operating systems (RTOSs), and therefore some stakeholders may view the use of CMDs in real-time contexts as incurring additional risk. While there may be additional risk, the characteristics of the operating systems themselves arguably can contribute less to that risk than the arbitrary workloads that may share computational resources with the medical software. Even traditional RTOSs are rarely able to make mathematically proven response time guarantees under any arbitrary, theoretical workload. Rather, real-time assurance is generated from some combination of proven-in-use (an RTOS has been used for many other real-time projects and can therefore be less risky than an operating system that has not been used in real-time projects), the use of well-understood and well-contained static workloads, the employment of fallback or graceful degradation mechanisms to reduce the impact of missed deadlines, and a heavy dose of empirical testing of the real-time software under a variety of workloads (including intentionally stressful workloads).

Mobile operating systems are subjected to a wide range of workloads across their user populations. Mobile operating system developers go to great lengths to help ensure that a single app, either accidentally or maliciously, is unable to dramatically degrade the user experience. For example, mobile device operating systems can limit the amount of execution resources available to background apps, so that the user's foreground activity remains responsive. It is increasingly difficult for any single app (either accidentally or maliciously) to starve other apps of computing resources. Finally, the response time of the diabetes use cases in the scope

of this guidance (usually measured in minutes) are far less stringent than the sub-millisecond response times required in other industrial real-time environments and well within the computing capabilities of modern CMDs.

For the remote-control use case, performance risk may be deemed minimal for CMDs. However, the solution can provide some out-of-band (distinct from the primary mobile operating system), assured feedback of the integrity of the remote-control operation to the user. For example, the insulin pump may provide audible, haptic, and/or visual feedback to the user that confirms the remote command, or the CMD can offer an alternative operating environment (e.g., hosted on a co-processor with exclusive display) to provide user confirmation of the command. Such an approach may provide additional security assurance as well.

The AID control use case typically involves real-time safety-critical software. The inability of CMD software to access required resources (including execution time, e.g., the ability to execute within the solution's required timeframe), without any additional failover mechanism, could render the solution unsafe. If a medical app were to utilize hardware-based secured execution environments, then the integrity of the operating system (and its scheduler) could be reduced as a source of risk as a hazard.

Resource requirements (including response time) will vary across implementations. For example, one implementation may require an autonomous treatment decision every five minutes and require 10 MB of random-access memory (RAM). Another may require a 30-min execution time interval. At time of this writing, response time windows are not less than a minute and RAM availability often plentiful and therefore well within the capability of modern CMDs, even under substantial load, assuming operating system integrity is intact. However, because the workload of CMDs may vary dramatically from user to user and be subjected to malicious denial of service attack by malware, one or more (ideally, all) of the following risk reduction mechanisms should be used:

— The developer should stress test and clinically test all supported CMDs and publish to all stakeholders the specific list of CMDs with configurations and operating systems that are deemed suitable, even under anomalous load, for AID use. Solutions should not be used on arbitrary, untested mobile devices.

— The developer should provide guidance to the user in the form of product documentation that can help reduce risk of real-time problems, such as (but not limited to) the avoidance of loading apps from untrusted sources or from unknown developers.

— Solutions should provide a failover mechanism such that missed real-time deadlines and other resource exhaustions can be detected by one or more of the solution's constituent regulated medical devices (e.g., insulin pump) and as a response to such failures, offer a method to exit autonomous operation and perform manual treatment.

4.1.4 Additional requirements to maintain availability of the personal area network (PAN)

This subclause only pertains to the AID control use case.

Ambulatory networks provide an increased quality of life to patients, but connectivity risks can be translated into patient risk if those networks are not resilient. CMDs in the context of this guidance are expected to be used within a wireless personal area network (PAN). Interconnectivity of component parts of the PAN and the connectivity of the PAN as a system to other networked entities like cloud services, electronic medical record systems, etc. are achieved by a number of communications transports and modalities. Industry standard radio frequency transports include IEEE 802.15.1™, IEEE 802.11™, and others, which exhibit great convenience during normal use but are susceptible to jamming, eavesdropping, and interference immunity threats. Some of these modalities provide some resilience features, such as frequency hopping, automatic reconnection after a service break, localized paired environment, etc. Generally speaking, however, consumer PANs are not currently designed to withstand sophisticated malicious attack of the physical network transport, in contrast to the resilient protocols used in some military wireless networks.

PAN denial of service should be considered in the context of medical use. Examples of failures that the PAN should be resilient to include, but are not limited to, the following:

— Deliberate jamming of PAN radio frequencies
— Failure of PAN radio transmissions due to hardware component failure
— Eavesdropping of PAN radio transmissions
— Radiated immunity threats from adjacent environments

In order to obtain sufficient resilience, at a minimum, the patient should be alerted and advised, if possible, when the system detects a risk to safety because of a failure of PAN communications.

This standard addresses additional concerns for three sub-use cases where a CMD is used to form part of a PAN. Many other use cases can be composed from combinations of the following three cases:

— The CMD acts as a "dumb terminal." It does nothing other than present data to the patient. The CMD does not act upon sensor input nor does it directly control medical operation. The CMD's disconnection from the PAN or failure to function properly can be tolerable for some time, and functionality can be replaced using a replacement CMD or backup display built-in to some other component of the PAN. In this case, the CMD not an essential component of the AID control system. Thus, loss of the CMD may create little or no significant risk to the patient.
— The CMD acts as a "headless" network element, passing through or routing communications, (e.g., from sensors to actuators elsewhere in the PAN) or enabling transmission of data from the PAN to a secure cloud service and back. Medical software is not resident on the CMD, and the CMD's failure to function properly or disconnection from the PAN can be tolerated for some well-defined time, depending on the clinical environment. In case of a PAN failure, the medically relevant sensors and/or actuators in the PAN may failover to an alternate, possibly degraded, mode without incurring significant patient risk. Such a mode may be invoked autonomously or require user intervention. In either case, the solution should make it clear to the patient that the solution is in a degraded configuration due to loss of the CMD. Full functionality can be regained with re-establishment of the CMD's operation within the PAN.
— The CMD acts as a smart controller through one or more dedicated software applications, and the PAN's sensors and actuators are merely authenticated components, possibly assembled through open procurement and communicating across standards-based interfaces and protocols (or even private or closed interfaces). This open system may consist of best of breed components selected by the system designer to create a PAN. The CMD and its smart medical software applications are responsible for critical communications and algorithmic control. While failed connection to the cloud may be tolerable, failure of the CMD within the PAN in this use case may be much more difficult to manage safely. In addition, malicious network-borne or malware-borne attacks add more risk to patient safety because the software's medical operation as well as failure detection (e.g., alarms that may alert the patient of a failure) may all be at risk of corruption and denial of service. Due to the risk of CMD failure, developers should avoid relying on the CMD exclusively for safe operation and consider employing redundant safety systems.

The developer should specify the amount of time necessary for the user to avoid, evade, and remediate any denial of service that can create an unacceptable risk to the user. The PAN-based solution should remain operable for the specified time period even during denial of service conditions.

The medically-relevant nodes at each end of an interrupted communication pathway within a PAN may announce their degraded communication to the user and/or other connected nodes of the PAN such that the user is alerted to a need to take action to remediate a loss of service that poses a risk to patient safety. Remediation