国 际 电 信 联 盟

ITU-T X.1331

(03/2018)

国际电信联盟
电信标准化部门

X系列：数据网、开放系统通信和安全性

安全应用和服务(2)– 智能电网安全

智能电网系统中家域网（HAN）设备的安全导则

ITU-T X.1331 建议书

国际电信联盟

ITU-T X 系列建议书

数据网、开放系统通信和安全性

公用数据网	X.1–X.199
开放系统互连	X.200–X.299
网间互通	X.300–X.399
报文处理系统	X.400–X.499
号码簿	X.500–X.599
OSI组网和系统概貌	X.600–X.699
OSI管理	X.700–X.799
安全	X.800–X.849
OSI应用	X.850–X.899
开放分布式处理	X.900–X.999
信息和网络安全	
一般安全问题	X.1000–X.1029
网络安全	X.1030–X.1049
安全管理	X.1050–X.1069
生物测定	X.1080–X.1099
安全应用和服务(1)	
组播安全	X.1100–X.1109
家庭网络安全	X.1110–X.1119
移动安全	X.1120–X.1139
网页安全	X.1140–X.1149
安全协议(1)	X.1150–X.1159
对等网络安全	X.1160–X.1169
网络身份安全	X.1170–X.1179
PITV安全	X.1180–X.1199
网络空间安全	
计算网络安全	X.1200–X.1229
反垃圾信息	X.1230–X.1249
身份管理	X.1250–X.1279
安全应用和服务(2)	
应急通信	X.1300–X.1309
泛在传感器网络安全	X.1310–X.1319
智能电网安全	**X.1330–X.1339**
验证邮件	X.1340–X.1349
物联网（IoT）安全	X.1360–X.1369
智能交通系统（ITS）安全	X.1370–X.1389
分布式账簿技术安全	X.1400–X.1429
安全协议(2)	X.1450–X.1459
网络安全信息交换	
网络安全综述	X.1500–X.1519
脆弱性/状态信息交换	X.1520–X.1539
事件/事故/探索法信息交换	X.1540–X.1549
政策的交换	X.1550–X.1559
探索法和信息要求	X.1560–X.1569
标示和发现	X.1570–X.1579
确保交换	X.1580–X.1589
云计算安全	
云计算安全综述	X.1600–X.1601
云计算安全设计	X.1602–X.1639
云计算安全最佳实践和指导原则	X.1640–X.1659
云计算安全实现	X.1660–X.1679
其他云计算安全	X.1680–X.1699

ITU-T X.1331 建议书

智能电网系统中家域网（HAN）设备的安全导则

摘要

智能电网中的家域网（HAN）是智能电网的一种驻地网络。与传统家域网不同，智能电网中的家域网包括分布式能源（DER）、电动汽车（EV）充电器、家庭能源管理系统（HEMS）和客户能源显示屏（CED）等智能电网设备。客户的用电负载和分布式能源（DER）与家域网相连，因此客户可以根据公用事业单位的信息打开或关闭负载和分布式能源，以便将电力的使用效率发挥到最大化。由于家域网通常与互联网相连，所以攻击者可轻易接入家域网和家域网设备。故而，家域网设备须提供阻止攻击者危害家域网及其设备的能力。ITU-T X.sgsec-2建议书草案将对智能电网中的家域网所面临的威胁进行分析，说明安全性要求和安全功能。由于每个家域网设备的作用和功能皆不相同，所以按设备分别介绍了它们的安全性要求和安全功能。

历史沿革

版本	建议书	批准日期	研究组	唯一识别码*
1.0	ITU-T X.1331	2018-03-29	17	11.1002/1000/13405

关键词

家域网、安全导则、安全性要求、智能电网

* 访问建议书，请在您的Web浏览器地址栏中输入网址http://handle.itu.int/，其次建议书的识别码，例如http://handle.itu.int/11.1002/1000/11830-en。

前言

国际电信联盟（ITU）是从事电信领域工作的联合国专门机构。ITU-T（国际电信联盟电信标准化部门）在电信，信息和通讯技术领域是国际电信联盟的常设机构。国际电信联盟电信标准化部门负责研究技术，操作和资费问题，并且为在世界范围内实现电信标准化，发表有关上述研究项目的建议书。

世界电信标准化大会（WTSA），每四年举行一次，确定ITU-T各研究组的研究课题，再由各研究组制定有关这些课题的建议书。

WTSA第一号决议规定了批准建议书须遵循的程序。

属ITU-T研究范围的某些信息技术领域的必要标准，是与国际标准化组织（ISO）和国际电工技术委员会（IEC）合作制定的。

注

本建议书为简明扼要起见而使用的“主管部门”一词，既指电信主管部门，又指经认可的运营机构。

遵守本建议书的规定是以自愿为基础的，但建议书可能包含某些强制性条款（以确保例如互操作性和适应性等），只有满足所有强制性条款的规定，才能达到遵守建议书的目的。“应该”或“必须”等其它一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

知识产权

国际电联提醒注意：本建议书的应用或实施可能涉及使用已申报的知识产权。国际电联对无论是其成员还是建议书制定程序之外的其它机构提出的有关已申报的知识产权的证据、有效性或适应性不表示意见。

至本建议书截止之日起，国际电联尚未收到实施本建议书可能需要的受专利保护的知识产权的通知。但需要提醒实施者注意的是，这可能并非最新消息，因此特大力提倡他们通过下列网址查询电信标准化局（TSB）的专利数据库：http://www.itu.int/ITU-T/ipr/。

目录

ITU-T X.1331建议书

智能电网系统中家域网（HAN）设备的安全导则

1 范围

本建议书提出智能电网系统中家域网（HAN）设备的安全导则。本建议书涵盖下列方面：

– HAN中设备的安全风险和通信；

– 对于HAN中设备和通信的安全性要求；

– HAN中设备和通信的安全功能。

2 参考文献

无。

3 术语和定义

3.1 它处定义的术语

本建议书使用了下列它处定义的术语：

3.1.1 能源服务界面（ESI）[b-ITU-T Y.2071]：由网关功能以及在用户驻地设备控制和管理智能电网服务的智能电网应用所需功能组成的一系列功能。

3.1.2 能源储存系统（ESS）[b-ITU-T L.1430]：能够存储或积累由能源生成器产生或从能源消费者那里捕获的能源的物理单元或部件。

注 – ESS为使用多种不同类型电池的提供电力储存功能。使用能源储存的一个示例是有效应对公用事业网络不断变化的价格机制。在用电成本相对较低阶段可以储存电能，从而可用得到储存的电能取代公用事业网络提供的更高价格的电力。

3.1.3 家域网（HAN）[b-ITU-T G.9959]：能够将家庭驻地的设备连接一起的网络。

3.1.4 家庭能源管理系统（HEMS）[b-ITU-T Y.4409]：包含有计算机平台的计算机系统，提供基本支持服务和一系列应用，或者提供家庭设备有效运行所需的功能性，这些家庭设备包括家用电器和存储电池，以确保以最低成本提供足够的能源安全性。

注 – HEMS在智能电网中由HAN指定。

3.1.5 家庭内显示器（IHD）[b-ITU-T Y.4409]：一种用户屏幕装置，目的是显示家庭能源消费信息。用户可利用这一可选功能通过其用户界面控制家庭中的设备。

注 – 控制和使用信息在HAN通信系统环境中传送。用户屏幕设备还可以是一部移动或智能电话、（互联网协议）电视、互联网视频电话、个人计算机、平板电脑或室内控制终端（wall-pad）。

3.1.6 广域网（WAN）[b-ITU-T Y.4409]：覆盖广泛地理区域的包含互联网的基于IP的通信网络，可容纳相关设备和局域网。

3.2 本建议书定义的术语

本建议书定义了下列术语：

3.2.1 电动汽车（EV）：可以通过任何外部电源进行反复充电的机动车，且同时可作为一种电力提供系统工作。

其中示例包括全电动汽车、电池EV、即插式混合EV和即插式混合EV改装产品。有时即插式EV称作电网驱动汽车或电力充电汽车。

3.2.2 邻域网（NAN）：有助于智能电网端点设备和家域网（HAN）与广域网（WAN）连接的接入网。

注 – 改编自[b-Smart-O-33]。

3.2.3 智能仪表：安装在驻地设备的一种装置，根据用户的需求响应信息，可对家庭智能设备的电力使用情况进行监督和控制。

注 – 改编自[b-ITU-T Y.4409]。

4 缩写词和首字母缩略语

本建议书使用以下缩写词和首字母缩略语：

AMI 先进计量基础设施
CED 客户能源显示器
DER 分布式电源
DG 分布式发电机
DoS 拒绝服务
DTLS 数据报传送层安全
ESI 能源服务界面
ESS 能源储存系统
EV 电动汽车
G/W 网关
HAN 家域网
HEMS 家庭能源管理系统
HMAC 基于散列技术的信息认证代码
ID 识别符
IP 互联网协议
IHD 家庭内显示器
NAN 邻域网
TLS 传送层安全
WAN 广域网
WPA 受Wi-Fi保护的接入

5 惯例

无。

6 智能电网中家域网的一般模型

智能电网是配备有信息通信技术的智慧电网。电力公用事业单位可利用智能电网根据通过智能电网收集到的用户用电信息，对电力需求做出估算，由此，公用事业单位可在估算基础上对高峰负荷情况予以控制。在电力负荷高峰出现前，公用事业单位可以减少客户的使用，或使客户转而采用由客户驻地分布式电源（DER）产生的备用电，如屋顶的太阳能光伏设备、储存电力或电动汽车（EV）。此外，客户可根据公用事业单位提供的高峰时段负荷信息推迟或提前用电。

为了在公用事业单位与客户之间交流信息，公用事业单位的估算数据或需求管理系统应连接至用户驻地设备，如家庭能源管理系统（HEMS）或客户能源显示器（CED）。图6-1具体说明智能电网环境中的多种不同网络。如该图所示，可经若干网络进行连接，如HAN、接入网[亦称作邻域网（NAN）]或（WAN）。

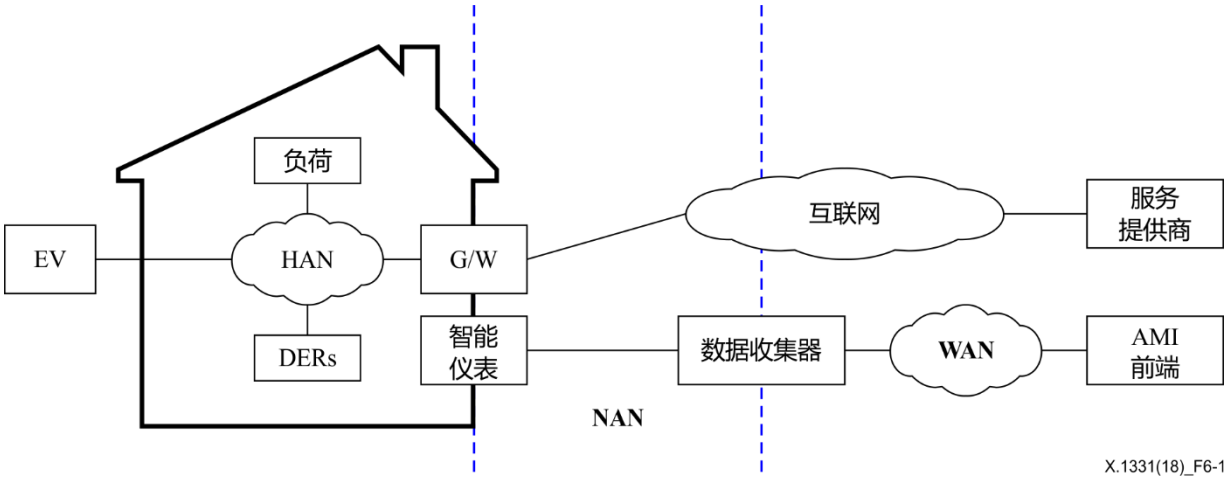

图6-1 – 智能电网中的多种不同类型网络

HAN将用户驻地的电力负荷和电力资源相连接。源自HAN设备的所有信息均应首先流向公用事业单位的后台系统（如从HAN到先进计量基础设施（AMI）前端）；公用事业单位提供的所有信息都应通过HAN提供至用户设备。

由于HAN通常与互联网相连，因此可通过互联网接入HAN。如果不怀好意的用户接入HAN，则通过HAN连接的设备会受到破坏，从而攻击者故意改变诸如电力负荷等信息。在这种情况下，攻击者可随意控制HAN设备。有鉴于此，应在通过HAN连接的设备中以及其相互通信中考虑到安全措施。

在具体说明威胁、要求和安全技术之前，应确立智能电网中HAN的一般模型。该一般模型应明确所有实体和相关通信界面，以澄清其相互之间的关系。

图6-2所示为智能电网中HAN的一般模型。在该HAN中，包含诸多成份，如电力负荷、DER、HEMS、CED（亦称作家庭内显示器（IHD））、能源服务界面（ESI）和智能仪表。

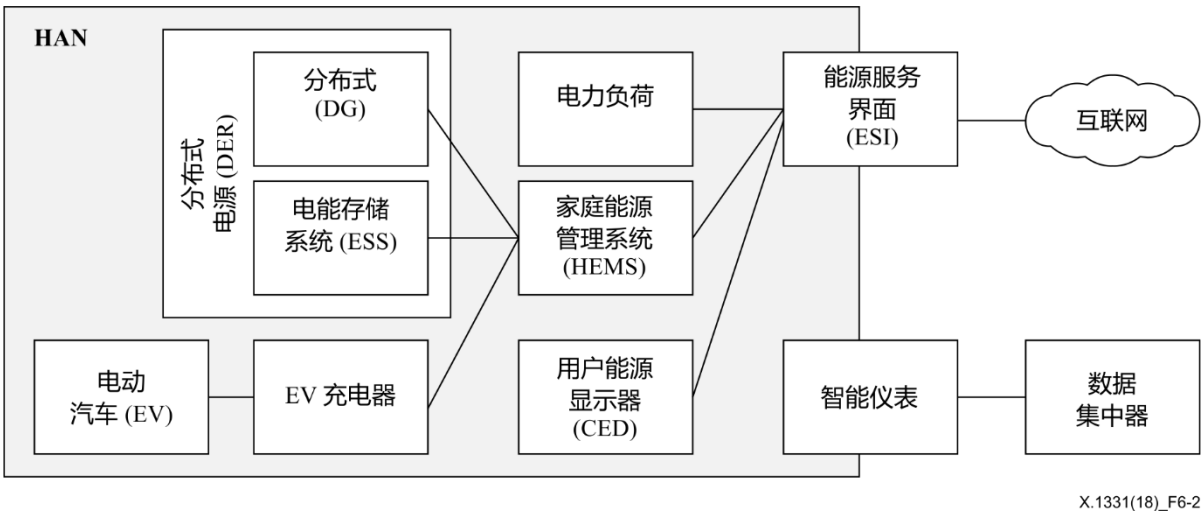

图6-2 – 智能电网中家域网的一般模型

- 电力负荷是诸如家用电器、空调和水泵等消耗电的装置产生的。通常负荷分为两类：智能和传统负荷。智能负荷包含传统负荷中不存在的通信和计量功能。尽管如此，由传统负荷产生的耗电可通过HEMS控制，条件是将智能插头插入插座中，前者具有通信和交换功能，因此，本建议书既阐明智能负荷，也阐明所谓电力负荷的智能插头。
- 包含分布式发电机（DG）和电力能源存储系统（ESS）的DER是为负荷提供电力的设备。HAN中的DG广泛采用太阳能光伏电源。
- EV既可以是负荷也可以是DER。对DER进行充电即构成了HAN中的负荷，但作为DER时它为家用电器提供电力。
- HEMS在客户登记的时间安排或预确定条件基础上，控制负荷功能和DER。条件的主要标准是建立价格和需求响应信号。
- CED显示当前电力使用统计数据和价格信息，从而使客户可以降低其电力消耗或改变其电力消费活动计划。

7 针对家域网安全威胁

本节讨论HAN面临的主要安全威胁。请注意，本节无意确定威胁的分类，但旨在阐明HAN运营商至少需要予以考虑的一些威胁。

7.1 数据泄露

人们普遍认为，存储和通信数据的披露是针对网络和设备的一种威胁。攻击者可积极主动偷听正在传送的数据，或实际接入某一设备，以获取其存储器中存储的数据。如果不对数据予以保护，则攻击者可对数据做出披露。

由于HAN中广泛采用无线通信，因此，可以轻而易举地在HAN内外进行偷听。此外，在许多情况下，HAN中的实体与互联网相连，因此，远程实体也可接入这些实体。由于这些原因，在HAN环境中，未得到授权的攻击者可以获得通信或存储数据。

在HAN中，诸如耗电信息、计费信息和电力使用计划等多种不同涉及隐私的信息存储在HEMS、CED或智能仪表中。这些私人数据可通过ESI在HEMS或CED中双向传送。数据泄露可对用户隐私带来严重负面影响。通过这些数据攻击者可以了解客户的日常生活规律。

此外，经通信网络，可将来自HEMS和CED的负荷、DER或EV充电器操作控制命令予以传送。攻击者通过获取数据即可知道如何控制HAN中的负荷和DER。对这种信息的了解可带来第7.2段所述的插入恶意数据等其它威胁。

7.2 伪造数据或插入恶意数据

未经授权的攻击者可插入、修改或删除HAN中实体之间或存储于HAN实体中的信息。攻击者可以是个人、程序或HAN实体。一旦出现这类威胁，数据完整性即遭到破坏。此外，破坏数据完整性还会导致设备运行不良。

由于无线通信网络可由任何匿名实体接入，因此，匿名实体可向HAN实体发送恶意数据。此外，攻击者还可向现有连接增加数据，目的是劫持连接或恶意发送数据。攻击者还可访问诸如HEMS等HAN实体的内存，从而改变存储数据或在内存中插入恶意数据。

如果电力价格信号调高，则HEMS可在违反用户意愿的情况下减少电力消费。此外，攻击者可控制信息，使EV或ESS不能充电。其它示例包括向实体发送大量请求，导致实体的拒绝服务（DoS）、改变数据文档中的数值或改变程序，以便使HAN实体以不同方式运行。

7.3 中断通信

中断通信的一种情况是通信堵塞 – 当有意或无意干扰力量超过通信链路的发送机或接收机力量时，即出现干扰，从而使通信链路瘫痪无用。另一个中断通信的示例是通过发送极大数量的数据过度消耗通信带宽。

在HAN中，HEMS应能收集与电力使用有关的负荷和DER状况信息，并从电力公用事业单位或服务提供商那里收到价格和控制信号，以便应对他们提出的调整要求。有鉴于此，为了使HAN运行正常，应当维护和完善其通信能力。

7.4 未经授权的接入

当攻击者获得诸如DER、HEMS或CED等实体的接入权时，即出现了未经授权的接入。攻击者假冒真实用户如此行事。一旦未经授权的接入获得成功，则攻击者亦可接入其它设备。

为了达到上述目的，攻击者必须得到识别和认证。为此，攻击者可进行端口扫描攻击，目的是找到HAN装置上具有漏洞的端口。如果存在具有漏洞的开放端口，则攻击者可充分利用该HAN设备的漏洞。此外，攻击者可以通过发起密码猜想攻击，以未经授权方式获得“无漏洞”服务。

恶意软件是另一种主要威胁。恶意软件可通过电子邮件或网络服务影响诸如CED等HAN设备，而且恶意软件还可扩散到HAN的其它装置中。一旦恶意软件安装在HAN设备中，即可在未经授权的情况下获得设备的资源，从而可能导致该设备运行不良、受损或中断运行。

7.5 可否认性

当作为发送方或接收方的攻击者否认已发送或接收信息时即出现该威胁。这不会导致HAN设备的损坏或运行不良，但发生该威胁时可能会引来冲突。根据冲突的性质，可能会导致无法正确确定服务故障或服务运行不良的原因。

7.6 安全威胁与家域网之间的关系

第7.1至7.5段所述的安全威胁会出现在HAN一般模型中的特定实体或通信中。表7-1所示为安全威胁与HAN实体之间的关系，其中小格中的空心圆表明具体实体存在的特定威胁。

表7-1 – 安全威胁与家域网之间的关系

实体	披露		修改/插入		中断	未经授权的接入	可否认性
	存储数据	通信数据	存储信息	通信信息			
负荷		○		○	○		
DER		○		○	○	○	○
EV充电器		○		○	○		○
HEMS	○	○	○	○	○	○	○
CED	○	○	○	○	○	○	○
ESI					○	○	
通信		○		○	○		

8 家域网安全要求

本节从安全的主要四个方面，即，可用性、保密性、完整性和不可否认性方面阐明高层安全要求。

8.1 可用性

可用性确保在发生影响网络的事件时，不会拒绝得到授权的对网元的接入以及对存储信息、信息流、服务和应用的获取。换言之，如果HAN中的一个实体希望在得到允许时在另一个设备上获得信息，则该实体应能立即接入所涉设备。

智能电网中的HAN应按照电网需求，控制负荷的使用以及DER的发电和电力储存。当公用事业单位估计已出现高峰需求，则应向HEMS或CED传送降低耗电请求或新的得到决定的价格信号，以便它们能够管理用户设备的电力需求。是否接受请求取决于客户登记的条件。

在这种情形下，首先必须保证网络的可用性和HAN实体的功能性。如果HAN网络在高峰需求出现时不可用，则可能使HEMS无法从公用事业单位那里收到任何信息，从而为客户带来更高成本。

8.2 保密性

保密性旨在确保未得到授权的实体不能读取数据内容。即便在出现以偷听方式在无线网上截获某些数据的情况，也可保证数据的保密性，除非攻击者不能对其予以显示。

实体和存储或传送敏感通信数据都需要保密性。HAN中的敏感数据包含电力使用计量信息、控制负荷和DER操作的命令信息、公用事业单位提出的价格信号或需求调整请求以及CED中的个人可识别信息。

8.3 完整性

完整性确保数据一旦传送即与源头数据保持一致。最近，数据完整性的含义得到扩大，涵盖了系统或设备状态，这对于不改变最初的基本配置是不可或缺的。同样，最初存储的数据也不能在经授权的操纵之后发生改变。

应确保控制命令以及HEMS与其它实体 – 负荷和DER – 之间传送的状态信息的完整性。此外，还应保护往返于CED的数据的完整性。同时，为了确保功能运行正常，安装在每一HAN设备中的程序清单以及程序本身都应得到保护。

8.4 不可否认性

不可否认性防止个人或实体否认已经进行了与数据相关的特定行动 – 提供有关行动的数字证据。

在HAN中，可能带来冲突的行动包括控制DER和负荷、接收价格信号和需求调整请求以及通过DER登记电力使用时间安排。因此，HAN中与这些行动有关的实体应满足不可否认性要求。然而在负荷方面，由于负荷的性能可能无法实现不可否认性。例如，智能插头是一个受到限制的装置，没有足够的内存或计算能力。

8.5 安全性要求与家域网之间的关系

表8-1表明安全性要求与安全威胁之间的关系，其中小格中的空心圆表示为了消除或减缓某一具体威胁而需得到满足的特定安全性要求。

表8-1 – 安全性要求与威胁之间的关系

			安全威胁						
			披露		修改/插入		中断	未经授权的接入	可否认性
			存储信息	通信信息	存储信息	通信信息			
安全性要求	保密性	存储数据	○						
		通信数据		○					
	完整性	存储数据			○			○	
		通信数据				○		○	
	可用性						○		
	不可否认性								○

由于表7-1列出了HAN中每一实体的威胁，且表8-1列出了针对每一威胁的要求，因此通过将这两个表相互关联，即可了解HAN中的每一实体的安全性要求。表8-2所示为HAN中各实体的安全性要求分配，其中小格中的空心圆表示每一实体应满足的特定安全性要求，以消除或减缓具体威胁。

表8-2 – 安全性要求在家域网实体中的分配

		安全性要求					
		可用性	保密性		完整性		不可否认性
			存储数据	通信数据	存储数据	通信数据	
实体	负荷	○		○		○	
	DER	○		○		○	○
	EV充电器	○		○		○	○
	CED	○	○	○	○	○	○
	HEMS	○	○	○	○	○	○
	ESI	○				○	
	通信	○		○		○	

9 安全要求和安全功能之间的关系

为满足HAN及其设备的安全要求，应使用安全功能。这些安全功能包括加密或解密、数字签名、消息认证、实体认证、授权、接入控制、反DoS攻击措施、审计和物理安全。表9-1描述了如何使用安全功能满足各项安全要求。方格中的圆圈表示可采用某一项安全功能满足具体的安全要求。请注意，表9-1所列各项安全功能的描述见第10节。

表9-1 – 安全要求与安全功能之间的关系

			安全功能							
			加密/解密	数字签名	认证		接入控制	反DoS	审计	物理安全
					消息	实体				
安全要求	保密性	存储数据	○							
		通信数据	○							
	完整性	存储数据		○	○		○			
		通信数据		○	○		○			
	可用性					○		○	○	○
	不可篡改性			○					○	○

10 智能电网系统内家域网设备的安全指南

10.1 用于负载的安全功能

表10-1列出了用于HAN负载的安全功能。该表显示了安全要求和安全功能之间的对应关系并详细描述了实施安全功能的各项能力。

表10-1 – 用于家域网负载的安全功能

安全 要求	安全 功能	描述
可用性	反DoS措施	应考虑检测和缓解DoS攻击的能力。
	物理安全	应考虑防止非授权物理接入的能力以便防止非授权用户操纵或配置负载。
完整性	消息认证	应考虑生成和认证数据加密完整性的能力以确保报告的完整性和对指令消息的控制。加密完整数据可由哈希运算消息认证码（HMAC）机制生成。
保密性	加密或解密	应考虑对HEMS指令消息进行解密和加密的能力。

10.2 用于分布式能源的安全功能

表10-2列出了HAN中DER的安全功能。该表显示出安全要求和安全功能之间的对应关系并详细阐述了实施安全功能的各项能力。

表10-2 – 用于家域网分布式能源的安全功能

安全要求	安全功能	描述
可用性	反DoS措施	应考虑检测和缓解DoS攻击的能力。
	物理安全	应考虑防止非授权物理接入的能力以便防止非授权用户操纵或配置DER。
完整性	消息认证	应考虑生成和认证加密完整性数据的能力以便确保报告和指令消息的完整性。加密完整性数据可由HMAC或数字签名机制生成。
	实体认证	• 应考虑发出控制指令消息的远程终端的认证能力。可将加密证书或证明的确认视为认证方法。 • 应考虑认证试图配置或操纵DER用户的能力。密码认证是典型的用户认证方式。可将生物特征，如手印，作为替代手段。
	接入控制	应考虑仅允许授权用户修改DER配置或进行操纵的能力。
保密性	加密或解密	应考虑对HEMS指令消息进行解密或加密的能力。
不可篡改性	数字签名	应考虑认证控制指令消息中数字签名的能力。
	审计	应考虑生成和维护审计跟踪的能力以便确保问责。ESS的充电和放电是一项应记录的重要行动。

10.3 用于电动汽车充电器的安全功能

表10-3列出了用于HAN中EV充电器的安全功能。该表显示出安全要求和安全功能之间的对应关系并详细阐述了实施安全功能的各项能力。

表10-3 – 用于家域网中电动汽车充电器的安全功能

安全要求	安全功能	描述
可用性	反DoS措施	应考虑检测和缓解DoS攻击的能力。
	物理安全	应考虑防止非授权物理接入的能力以便防止非授权用户操纵或配置充电器。
完整性	消息认证	应考虑生成和认证加密完整性数据的能力以便确保报告和指令消息的完整性。加密完整性数据可由HMAC或数字签名机制生成。
	实体认证	• 应考虑发出控制指令消息的远程终端的认证能力。可将加密证书或证明的确认视为认证方法。 • 应考虑认证试图配置或操纵DER用户的能力。密码认证是典型的用户认证方式。可将生物特征，如手印，作为替代手段。
	接入控制	应考虑仅允许授权用户修改充电器配置或进行操纵的能力。
保密性	加密或解密	应考虑对HEMS指令消息进行解密或加密的能力。
不可篡改性	数字签名	应考虑认证控制指令消息中数字签名的能力。
	审计	应考虑生成和维护审计跟踪的能力以便确保问责。启动或停止充电是应记录的一项重要行动。

10.4 用于客户能源显示器的安全功能

表10-4列出了HAN中CED的安全功能。该表显示出安全要求和安全功能之间的关系并详细阐述了实施安全功能的各项能力。

表10-4 – 家域网中客户能源显示器的安全功能

安全要求	安全功能	描述
可用性	物理安全	应考虑防止非授权物理接入的能力以便防止非授权用户操纵或配置CED。
完整性	消息认证	应考虑生成和认证加密完整性数据的能力以便确保报告和指令消息的完整性。加密完整性数据可由HMAC或数字签名机制生成。
	实体认证	• 应考虑认证HEMS的能力。证书的认证可视为一种认证方法。 • 应考虑认证试图使用CED的用户的能力。密码认证是典型的用户认证方式。可将生物特征，如手印，作为替代手段。

表10-4 – 家域网中客户能源显示器的安全功能

	接入控制	应考虑仅允许授权用户修改CED认证或其功能的能力。
	应用完整性	应考虑确保应用完整性的能力以便检测由恶意软件影响的或攻击方修改的应用。攻击者可修改或故意删除可执行文件或文件库，从而造成应用不稳定。使用这一能力，HAN设备可确定应用是否更改。该能力的一个方法示例就是对应用加密完成代码的认证，该代码是在应用安装或更新时生成的。
保密性	加密或解密	• 应考虑加密或解密来自于或发送至HEMS的消息的能力以便保护指令消息和包含个人可识别信息的消息。 • 应考虑加密或解密存储在CED中的数据的能力以便保护CED中个人可识别信息。
不可篡改性	数字签名	应考虑认证包含在控制指令中的数字签名的能力。
	审计	应考虑创建和维护审计跟踪的能力以便确保问责。

10.5 有关家庭能源管理系统的安全功能

表10-5列出了HAN中HEMS的安全功能。该表显示出安全要求和安全功能之间的对应关系并详细阐述了实施安全功能的各项能力。

表10-5 – 家域网中家庭能源管理系统的安全功能

安全要求	安全功能	描述
可用性	反DoS措施	应考虑检测和缓解DoS攻击的能力，特别是当客户使用一项服务控制负载时，应保护DER免受DoS攻击。
	物理安全	应考虑防止非授权物理接入的能力以便防止非授权用户使用HEMS。
完整性	消息认证	应考虑生成和认证加密完整性数据的能力以便确保来自其他设备（负载、DER和EV充电器）以及发送至其他设备（负载、DER和EV充电器）的控制指令的状态信息的完整性。加密完整性数据可由HMAC或数字签名机制生成。
	实体认证	• 应考虑认证远程终端的能力。证书的认证可视为一种认证方法。对于计算功率较低的负载，可通过认证基于预分享的机密而生成的证书予以实现。 • 应考虑认证试图使用HEMS的用户的能力。密码认证是一项用户认证的典型方法。生物特征和快速反应代码可作为替代方法。
	接入控制	仅允许授权用户更改HEMS配置并使用其功能的能力。管理员和普通用户的账户应分开。应为不同目的设立并使用不同的账户，使攻击者只能有限地获得敏感信息、功能和其他账户（在一个账户受到破坏的情况下）。

表10-5 – 家域网中家庭能源管理系统的安全功能

安全要求	安全功能	描述
	应用完整性	应考虑确保应用完整性的能力以便检测由恶意软件影响的或攻击方修改的应用。攻击者可修改或故意删除可执行文件或文件库，从而造成应用不稳定。使用这一能力，HAN设备可确定应用是否更改。该能力的一个方法示例就是对应用加密完成代码的认证，该代码是在应用安装或更新时生成的。
保密性	加密或解密	• 应考虑解密或加密来自于或发送至HEMS的消息的能力以便保护指令消息和包含个人可识别信息的消息。 • （如需要）应考虑加密或解密存储在CED中的数据的能力以便保护CED中个人可识别信息。
不可篡改性	数字签名	应考虑认证包含在控制指令中的数字签名的能力。
	审计	应考虑创建和维护审计跟踪的能力以便确保问责。

10.6 有关能源服务界面的安全功能

表10-6列出了HAN中ESI的安全功能。该表显示出安全要求和安全功能之间的对应关系并详细阐述了实施安全功能的各项能力。

表10-6 – 家域网中能源服务界面的安全功能

安全要求	安全功能	描述
可用性	物理安全	应考虑防止非授权物理接入的能力以便防止非授权用户使用ESI。
完整性	接入控制	• 应考虑仅允许授权本地设备接入HAN的能力。对于Wi-Fi接入点，应采用受Wi-Fi保护的接入（WPA）II并使密码复杂化从而防止密码猜测攻击。此外，应关闭服务套件标识码（ID）广播功能。对于Zigbee或蓝牙接入点，每项协议规范中的安全功能应得到全面实施以便满足安全要求。 • 应考虑基于独一无二的ID阻挡非授权流量的能力。设备的媒体接入控制（MAC）地址或互联网协议（IP）地址可作为独一无二的ID使用。
	应用完整性	应考虑确保应用完整性的能力以便检测由恶意软件影响的或攻击方修改的应用。攻击者可修改或故意删除可执行文件或文件库，从而造成应用不稳定。使用这一能力，HAN设备可确定应用是否更改。该能力的一个方法示例就是对应用加密完成代码的认证，该代码是在应用安装或更新时生成的。

10.7 有关通信的安全功能

表10-7列出了HAN中通信的安全功能。该表显示出安全要求和安全功能之间的对应关系并详细阐述了实施安全功能的各项能力。

表10-7 – 家域网中通信的安全功能

安全要求	安全功能	描述
可用性	反DoS措施	应考虑检测和缓解DoS攻击的能力。
完整性	消息/实体认证	应考虑相互认证通信实体和消息的能力以便确保通信数据的完整性。使用证书的传送层安全（TLS）或数据报文传送层安全（DTLS）可作为适当的选择。应为TLS或DTLS选择适当的安全加密算法。
	接入控制	• 应考虑仅允许授权本地设备接入HAN的能力。 • 应考虑基于独一无二的ID阻挡非授权流量的能力。设备的MAC地址或IP地址可用作独一无二的ID。
保密性	加密或解密	应考虑对HEMS存储数据进行加密或解密的能力以便在必要时对HEMS中的个人可识别信息提供保护。

参考资料

[b-ITU-T G.9959] Recommendation ITU-T G.9959 (2015), Short range narrow-band digital radiocommunication transceivers – PHY, MAC, AR and LLC layer specifications.

[b-ITU-T L.1430] Recommendation ITU-T L.1430 (2013), *Methodology for assessment of the environmental impact of information and communication technology greenhouse gas and energy projects*.

[b-ITU-T Y.2071] Recommendation ITU-T Y.2071 (2015), *Framework of a micro energy grid.*

[b-ITU-T Y.4409] Recommendation ITU-T Y.4409/Y.2070 (2015), *Requirements and architecture of the home energy management system and home network services*.

[b-ITU-T Smart-O-33] ITU-T FG-Smart Grid: Smart-O-33Rev.6 (2011), *Smart grid architecture*;
http://www.itu.int/en/ITU-T/focusgroups/smart/Documents/smart-o-0033r6_architecture_deliverable.doc

ITU-T 系列建议书

A系列	ITU-T工作的组织
D系列	一般资费原则
E系列	综合网络运行、电话业务、业务运行和人为因素
F系列	非话电信业务
G系列	传输系统和媒质、数字系统和网络
H系列	视听及多媒体系统
I系列	综合业务数字网
J系列	有线网络和电视、声音节目及其它多媒体信号的传输
K系列	干扰的防护
L系列	环境与ICT、气候变化、电子废物、节能；线缆和外部设备其他组件的建设、安装和保护
M系列	电信管理，包括TMN和网络维护
N系列	维护：国际声音节目和电视传输电路
O系列	测量设备的技术规范
P系列	电话传输质量、电话设施及本地线路网络
Q系列	交换和信令
R系列	电报传输
S系列	电报业务终端设备
T系列	远程信息处理业务的终端设备
U系列	电报交换
V系列	电话网上的数据通信
X系列	**数据网、开放系统通信和安全性**
Y系列	全球信息基础设施、互联网协议问题、下一代网络、物联网和智慧城市
Z系列	用于电信系统的语言和一般软件问题

瑞士印刷
2018年，日内瓦