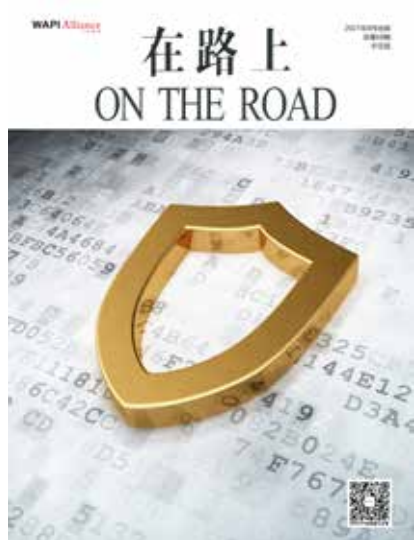


在路上 ON THE ROAD





WAPI产业联盟

理 事 长： 曹 军

秘 书 长： 张璐璐

《在路上 On The Road》编辑部

主 编： 张璐璐

编 辑： 周 园 刘 婷 简 练
 王立华 肖 非 刘剑昕

美术编辑： 周 园

WAPI产业联盟秘书处

会员服务部 标 准 化 部 市场与产业部
测试实验室 综合管理部

联络单位

ISO/IEC JTC1/SC6中国对口委员会
工业和信息化部宽带无线IP标准工作组

联系方式

地 址： 北京海淀区知春路27号量子芯座1608室

邮 编： 100191

电 话： 010-82351181

传 真： 010-82351181 ext.1901

邮 箱： wapi@wapia.org zhoyu@wapia.org

网 站： <http://www.wapia.org.cn>

公众号：



WAPI产业联盟公众号

理事成员：

中国移动通信集团公司

中国电信集团有限公司

中国联合网络通信集团有限公司

国家密码管理局商用密码检测中心

国家无线电监测中心检测中心

北大方正集团有限公司

北京中电华大电子设计有限责任公司

北京六合万通微电子技术有限公司

广州杰赛科技股份有限公司

西安西电捷通无线网络通信股份有限公司

深圳市明华澳汉科技股份有限公司

媒体聚焦 Media Focus

- 05 中国电子报等：WAPI产业联盟发布新版测试项 助力行业新基建
- 07 通信世界等：ISO/IEC JTC 1/SC 6/WG 7召开中期会议 我国4项国际标准提案获推进
- 09 信安标委、密码君等：我国SM4分组密码算法正式成为ISO/IEC国际标准

特别报道 Special Report

- 14 南网首个“云巢”搭建成功 WAPI应用到无人机作业领域 保障数据安全传输
- 15 《党委（党组）网络安全工作责任制实施办法》解读
- 19 浅谈我国商用密码标准体系

联盟关注 Alliance Concerns

- 22 联盟人谈标准创新系列（三）刘 婷：标准领航，助力关键信息基础设施安全防护建设

政经要闻 Policy News

- 28 工信部：就网络安全产业高质量发展三年行动计划（2021-2023年）征求意见
- 28 网信办：数字中国建设要统筹发展与安全
- 29 网信办：就《网络安全审查办法(修订草案)》征求意见
- 29 肖亚庆：大力发展网络安全产业将有效推动数字经济高质量发展
- 29 田世宏：务实推进网络安全标准化工作高质量发展
- 30 赵泽良：网络安全标准要服务国家发展战略大局
- 30 谢永泉：全面贯彻落实《密码法》 依法推进商用密码创新发展

联盟工作 Alliance Work

- 31 联盟秘书处组织收看“庆祝中国共产党成立100周年大会盛况现场直播”
- 32 联盟秘书处系统学习中国共产党党史
- 34 联盟秘书处认真学习贯彻习总书记在两院院士大会 中国科协十大上的重要讲话精神
- 35 WAPI产业联盟召开2021年第一次理事会和监事会
- 36 WAPI产业联盟召开2021年会员大会（总第十五次）
- 38 WAPI产业联盟召开2021年第二次标准工作及项目组会议（总第118次）
- 40 WAPI产业联盟3项无线局域网系统/工程团体标准正式立项
- 41 WAPI产业联盟2项无线局域网接入控制团体标准进入送审阶段
- 42 WAPI产业联盟成为北京市地方标准《高质量团体标准评价指标体系》联合起草单位
- 43 WAPI产业联盟组织会员参加 2021“科创中国”科技创新企业家高峰论坛
- 45 南网深圳数研院WAPI系列产品通过联盟测试
- 46 西电捷通公司国产平台WAPI鉴别服务器通过联盟测试
- 46 西电捷通公司WAPI无线接入鉴别综合网关通过联盟测试

成员与市场 Member & Marketing

- 47 华信傲天发布高性能无线局域网接入点产品
- 48 迈普通信以双第一中标中国电信集采
- 48 新华三中标中国移动高端路由器和高端交换机集采项目
- 49 数字认证蝉联“中国网络安全百强”领军者行列
- 49 华为最大的网络安全透明中心启用
- 50 美国国土安全部将发布首份管路系统网络安全指令文件

WAPI 产业应用论坛 WAPI Forum

- 52 航天科创：基于WAPI的变电站多光谱智能巡检系统

中国电子报等：

WAPI产业联盟发布新版测试项 助力行业新基建

【编者按】2021年7月20日，WAPI产业联盟发布了《无线局域网鉴别与保密基础结构（WAPI）功能测试项目（2021年7月版）》（以下简称《新版WAPI测试项》）。这与近期发布的《无线局域网产品工程化实现指南 第10部分：WAPI与IEEE 802.11ax》、《管理帧保护技术规范》等团体标准和技术指标密切贴合，目的是更好地服务各行各业高质量WAPI建设。目前，联盟实验室已依据《新版WAPI测试项》实施WAPI产品测试，为市场用户的WAPI采购、验收、监督检查等提供支撑。

中国电子报/电子信息产业网、通信世界、飞象网等媒体第一时间发布了相关报道。

以下中国电子报/电子信息产业网的报道。



日前，WAPI产业联盟发布了《无线局域网鉴别与保密基础结构（WAPI）功能测试项目（2021年7月版）》（以下简称《新版WAPI测试项》）。这与近期发布的《无线局域网产品工程化实现指南 第10部分：WAPI与IEEE 802.11ax》、《管理帧保护技术规范》等团体标准和技术指标密切贴合，目的是更好地服务各行各业高质量WAPI建设。目前，联盟实验室已依据《新版WAPI测试项》实施WAPI产品测试，为市场用户的WAPI采购、验收、监督检查等提供支撑。

相较联盟上一版测试项，首先，《新版WAPI测试项》在终端STA、无线接入点AP、鉴别服务器AS三大类测试对象的基础上，新增了证书签发服务器（CIS）这一测试对象。其次，新增了WAPI与11ax互通性测试，以及管理帧保护（单播）连通性测试、终端实体证书管理（CMEE）及私钥生成方式测试、同一ASU域内AP间切换时延测试等多项扩展功能测试。通过这些新测试，能够满足当前各行业关键信息基础设施建设的更高要求。



无线局域网鉴别与保密基础结构（WAPI）功能测试项目（2021年7月版）

而相较于其他WAPI基础合规性测试，WAPI产业联盟开展的无线局域网鉴别与保密基础结构（WAPI）功能测试，具有测试项目更全面、测试颗粒度更细、测试结果更能精准贴合用户高质量WAPI建设需求、定制化程度更高等特点。更值得一提的是，联盟开展的WAPI测试，与无线局域网技术创新演进保持同步，例如：《新版WAPI测试项》中增加了对管理帧保护功能的测试，可有效防止当前某些攻击者通过持续发送解除关联和解除链路验证等消息导致用户无法接入网络或强制用户下线的情况；又如：对终端实体证书管理（CMEE）及私钥生成功能的测试，用户可自主生成密钥并在线获取证书，实现证书自动下载和更新，证书管理的便捷性大大提高。

当下，WAPI产业联盟正进一步发挥创新联合体优势，通过公共技术服务等平台，去解决用户高质量WAPI建设中的技术难题、产品难题、工程难题等。因专业性、中立性和开放性，让越来越多的市场用户信任联盟，采用“委托联盟开展测试”、“采信联盟测试报告”等方式，协助用户WAPI产品选型和市场建设。此外，市场用户和联盟协同开展的标准化、产业化、检测校验等创新工作也正在推进中。

部分媒体新闻链接：

中国电子报/电子信息产业网：<http://www.cena.com.cn/infocom/20210721/112572.html>

通信世界：<http://www.cww.net.cn/article?id=488872>

飞象网：<http://www.cctime.com/html/2021-7-20/1582108.htm>

通信世界等：

ISO/IEC JTC 1/SC 6/WG 7召开中期会议 我国4项国际标准提案获推进

【编者按】2021年7月6-9日，国际标准化组织（ISO）和国际电工委员会（IEC）第一联合技术委员会（JTC 1）第六分技术委员会（SC 6）第七工作组（WG 7）召开中期会议，来自中国、韩国、英国、美国、西班牙的16位专家参加了会议。WAPI产业联盟秘书处张璐璐、简练等同志和无线网络安全标准化委员会相关同志作为中国代表团专家参会。中国代表团主导/参与的4项国际标准提案获顺利推进。

通信世界、飞象网等媒体对此进行了报道。

以下是通信世界的报道。



通信世界消息（CWW）2021年7月6-9日，国际标准化组织（ISO）和国际电工委员会（IEC）第一联合技术委员会（JTC 1）第六分技术委员会（SC 6）第七工作组（WG 7）召开中期会议，来自中国、韩国、英国、美国、西班牙的16位专家参加了会议。WAPI产业联盟秘书处张璐璐、简练等同志和无线网络安全标准化委员会相关同志作为中国代表团专家参会。

会议期间，进行了ISO/IEC 21558 “未来网络架构”和ISO/IEC 21559 “未来网络协议和机制”系列国际标准项目投票意见处理会议（CRM），并审议了WG 7在研国际标准项目的最新情况。中国代表团主导/参与的4项国际标准提案获顺利推进。

其中，由中国电信、WAPI产业联盟、西电捷通和新华三于2020年5月新立项的“无线局域网接入控制”（ISO/IEC 5021-1和ISO/IEC 5021-2）两项提案于会前提交了更新的工作草案（WD），会上审议并修改了工作草案，计划在8-9月SC 6全会上提请进入委员会草案（CD）投票。由重庆邮电大学牵头制定的“基于代理模型的服务质量”（ISO/IEC 21558-2和ISO/IEC 21559-2）两项提案，会上完成了对CD投票意见的处理，已进入国际标准草案（DIS）阶段。

ISO/IEC JTC 1/SC 6是信息技术领域国际标准化组织重要的分技术委员会，其技术方向为系统间远程通信和信息交换，专注于开放系统之间信息交换领域的技术研究和标准化，涵盖国际标准化组织提出的开放系统互联（OSI）七层模型，是全球网络空间系统信息通信的基础。目前，WAPI产业联盟组织会员单位推进并获发布的14项ISO/IEC国际标准中，有8项是在ISO/IEC JTC 1/SC 6制定的。

部分媒体新闻链接：

通信世界：<http://www.cww.net.cn/article?id=488941>

中国电子报/电子信息产业网：<http://m.cena.com.cn/infocom/20210721/112574.html>

飞象网：<http://www.cctime.com/html/2021-7-21/1582372.htm>

信安标委、密码君等：

我国SM4分组密码算法正式成为ISO/IEC国际标准

【编者按】一项技术标准的产业化和应用程度，是其被采纳为国际标准的重要考量依据。

WAPI是采用了我国首个公开的商用密码算法SM4且产业化市场化程度很高的自主创新技术。早在2006年，国家密码管理局发布第7号公告，批准无线局域网产品使用SM4分组密码算法（当时名称为SMS4）。伴随着WAPI大规模产业化和应用，SM4已成为我国首个大批量进入通信产业/国际市场的国产算法，在全球已实现了百亿级芯片产量。

2021年6月，SM4算法获ISO/IEC国际标准组织正式发布。安全标准化技术委员会、国家密码管理局、搜狐网、网易等对此事发布了相关报道。

以下是信安标委和密码君的新闻节选。



2021年6月25日，我国SM4分组密码算法作为国际标准ISO/IEC 18033-3:2010/AMD1:2021《信息技术 安全技术 加密算法 第3部分：分组密码 补篇1：SM4》，由国际标准化组织ISO/IEC正式发布。

ISO/IEC 18033-3:2010包含了64位分组密码算法（TDEA、MISTY1、CAST-128、HIGHT）和128位分组密码算法（AES、Camellia、SEED），新发布的补篇主要包含我国的SM4分组密码算法。SM4作为ISO/IEC标准发布标志着我国商用密码算法国际标准体系进一步完善，展现了我国先进的密码科技水平和国际标准化能力，对提升我国商用密码产业发展、推动商用密码更好服务“一带一路”建设具有重要意义。

我国于2016年10月正式提交关于SM4算法纳入ISO/IEC 18033-3的国际标准提案，后立项为国际标准研究项目启动研究；2017年4月，SM4算法作为ISO/IEC 18033-3补篇正式立项，启动标准编制工作；2021年6月标准文本正式发布。我国2名专家担任该补篇的编辑和联合编辑。

■ 我国密码算法国际化进程

《密码法》第二十三条第一款规定：国家推动参与商用密码国际化活动，参与制定商用密码国际标准，推进商用密码中国标准与国外标准之间的转化运用。

我国高度重视商用密码国际化工作，大力推进以我国自主设计研制的SM系列密码算法为代表的中国商用密码标准纳入国际标准，积极参与国际化活动，加强国际交流合作。

01 2011年9月，我国设计的祖冲之(ZUC)算法纳入国际第三代合作伙伴计划组织(3GPP)的4G移动通信标准，用于移动通信系统空中传输信道的信息加密和完整性保护，这是我国密码算法首次成为国际标准。

2017年，SM2和SM9数字签名算法正式成为ISO/IEC国际标准。

2018年，SM3算法正式成为ISO/IEC国际标准。

2020年4月，ZUC序列密码算法正式成为ISO/IEC国际标准。

2021年2月，SM9标识加密算法正式成为ISO/IEC国际标准。

2021年6月，SM4分组密码算法正式成为ISO/IEC国际标准。

02 我国商用密码国际标准体系已初步成型，为密码在全球范围的发展与应用提供了中国方案,贡献了中国智慧。

■ SM4加密算法详解

1 SM4分组密码算法概述

(1) SM4密码算法是我国自主设计的分组对称密码算法，用于实现数据的加密/解密运算，以保证数据和信息的机密性。

(2) 该算法的分组长度为128比特，密钥长度为128比特。

(3) 加密算法与密钥扩展算法都采用32轮非线性迭代结构。

(4) SM4通过加密密钥生成轮密钥，通过轮密钥进行加解密运算。

(5) 数据解密和数据加密的算法结构相同，只是轮密钥的使用顺序相反，解密轮密钥是加密轮密钥的逆序。

2 SM4分组密码算法优点

SM4 算法具有安全高效的特点，在设计和实现方面具有以下优势：

(1) 在设计上实现了资源重用，密钥扩展过程和加密过程类似。

(2) 加密过程与解密过程相同，只是轮密钥使用顺序正好相反，它不仅适用于软件编程实现，更适合硬件芯片实现。

(3) 轮变换使用的模块包括异或运算、8比特输入8比特输出的S盒，还有一个32比特输入的线性置换，非常适合 32 位处理器的实现。

通过对 SM4 密码算法的安全性分析结果表明：SM4 算法的 S 盒设计具有较高的安全特性，线性置换的分支数达到了最优，可以抵抗差分分析、线性分析、代数攻击等密码分析方法。

在安全性上，SM4 算法的密钥长度是 128 比特，其安全性与 AES-128 是相当的(AES还支持更高的安全强度)。在实现效率方面，由于SM4 密钥扩展和加密算法基本相同，且解密时可以使用同样的程序，只需将密钥的顺序倒置即可，因此 SM4 算法实现起来较为简单；而AES算法的加密算法与解密算法不一致，实现起来更复杂一些。

3 SM4预备知识

(1) SM4术语解释

1: 字与字节：字节是内存的基本单位，一个字节由8个比特组成，一个字等于4个字节，由32个比特组成。

2: $\oplus$ ：32比特异或运算

3: $\ll i$ ：循环左移*i*比特运算

4: s盒：固定的8比特输入8比特输出置换，记为Sbox (.)。

SM4 算法说明--S盒

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	d6	90	e9	fe	cc	e1	3d	b7	16	b6	14	c2	28	fb	2c	05
1	2b	67	9a	76	2a	be	04	c3	aa	44	13	26	49	86	06	99
2	9c	42	50	f4	91	ef	98	7a	33	54	0b	43	ed	cf	ac	62
3	e4	b3	1c	a9	c9	08	e8	95	80	df	94	fa	75	8f	3f	a6
4	47	07	a7	fc	f3	73	17	ba	83	59	3c	19	e6	85	4f	a8
5	68	6b	81	b2	71	64	da	8b	f8	eb	0f	4b	70	56	9d	35
6	1e	24	0e	5e	63	58	d1	a2	25	22	7c	3b	01	21	78	87
7	d4	00	46	57	9f	d3	27	52	4c	36	02	e7	a0	c4	c8	9e
8	ca	bf	8a	d2	40	e7	38	b5	a3	f7	f2	ce	f9	61	15	a1
9	e0	ae	5d	a4	9b	34	1a	55	ad	93	32	30	f5	8e	b1	e3
a	1d	f6	e2	2e	82	66	ca	60	e0	29	23	ab	0d	53	4e	6f
b	d5	db	37	45	de	fd	8e	2f	03	ff	6a	72	6d	6c	5b	51
c	8d	1b	af	92	bb	dd	bc	7f	11	d9	5c	41	1f	10	5a	d8
d	0a	c1	31	88	a5	cd	7b	bd	2d	74	d0	12	b8	e5	b4	b0
e	89	69	97	4a	0c	96	77	7e	65	b9	f1	09	c5	6e	c6	84
f	18	f0	7d	ec	3a	dc	4d	20	79	ee	5f	3e	d7	cb	39	48

输入“EF”，则经S盒后的值为表中第E行和第F列的值，Sbox (EF) =84

(2) 轮函数F

采用非线性迭代结构，以字为单位进行加密运算，称一次迭代运算为一轮变换。轮函数F为

$$F(X_0, X_1, X_2, X_3, rk) = X_0 \oplus T(X_1 \oplus X_2 \oplus X_3 \oplus rk)$$

(3) 合成置换T

T: 从一个字转换为另一个字，是一个可逆变换，由非线性变换 τ 和线性变换L复合而成，即 $T(.) = L(\tau(.))$ 。

a.非线性变换 τ : τ 由4个并行的S盒构成。设输入为 $A = (a_0, a_1, a_2, a_3)$ ，其中 a_0, a_1, a_2, a_3 均为字节类型，输出为 $B = (b_0, b_1, b_2, b_3)$ ，其中 b_0, b_1, b_2, b_3 均为字节类型，则：

$$(b_0, b_1, b_2, b_3) = \tau(A) = (Sbox(a_0), Sbox(a_1), Sbox(a_2), Sbox(a_3))$$

非线性就是离散的，无规律的，没有公式可以描述的。

b.线性变换L: 非线性变换 τ 的输出是线性变换L的输入。设输入为B，B是一个字，输出为C，C是一个字，则：

$$C = L(B) = B \oplus (B \lll 2) \oplus (B \lll 10) \oplus (B \lll 18) \oplus (B \lll 24)$$

4 加解密算法

定义反序变换R为: $R(A_0, A_1, A_2, A_3) = (A_3, A_2, A_1, A_0)$ 。所有A均为字，即: unsigned int。

设明文输入为 (X_0, X_1, X_2, X_3) ，所有 X_i 均属于字，整体为一个具有4个元素的字数组，密文输出为 (Y_0, Y_1, Y_2, Y_3) ，所有 Y_i 均属于字，整体为一个具有4个元素的字数组，轮密钥为 $rk_0, rk_1, rk_2 \dots rk_{31}$ ，所有 rk_i 均属于字，整体为一个具有32个元素的字数组。

则本算法的加密变换为：

$$X(i+4) = F(X_i, X(i+1), X(i+2), X(i+3), rk_i) = X_i \oplus T(X(i+1) \oplus X(i+2) \oplus X(i+3) \oplus rk_i)$$

i的取值0,1,2...31

$$(Y_0, Y_1, Y_2, Y_3) = R(X_{32}, X_{33}, X_{34}, X_{35}) = (X_{35}, X_{34}, X_{33}, X_{32})$$

算法的解密变换与加密变换结构相同，不同的仅是轮密钥的使用顺序。

加密时轮密钥的使用顺序为: $(rk_0, rk_1, \dots, rk_{31})$;

解密时轮密钥的使用顺序为: $(rk_{31}, rk_{30}, \dots, rk_0)$

5 密钥扩展算法

本算法中加密算法的轮密钥由加密密钥通过密钥扩展算法生成。

加密密钥 $MK = (MK_0, MK_1, MK_2, MK_3)$ ， MK_i 均属于32比特的字， $i=0,1,2,3$;

令 K_i 属于32比特的字, $i=0,1,\dots,35$, 轮密钥为 r_{ki} 属于32比特的字, $i=0,1,2,\dots,31$ 。则轮密钥生成方法为:

首先,

$$(K_0, K_1, K_2, K_3) = (MK_0 \oplus FK_0, MK_1 \oplus FK_1, MK_2 \oplus FK_2, MK_3 \oplus FK_3)$$

然后对 $i=0,1,2,\dots,31$:

$$r_{ki} = K(i+4) = K(i) \oplus T'(K(i+1) \oplus K(i+2) \oplus K(i+3) \oplus CK(i))$$

(1) T' 变换与加密算法轮函数中的 T 基本相同, 只将其中的线性变换 L 修改为以下 L' :

$$L'(B) = B \oplus (B \lll 13) \oplus (B \lll 23)$$

(2) 系统参数 FK 的取值, 采用16进制表示为: $FK_0=(A3B1BAC6)$, $FK_1=(56AA3350)$, $FK_2=(677D9197)$, $FK_3=(B27022DC)$ (3) 固定参数 CK 的取值方法为: 设 $ck(i,j)$ 为 CK_i 的第 j 字节($i=0,1,\dots,31$; $j=0,1,2,3$), 即 $CK_i=(ck(i,0), ck(i,1), ck(i,2), ck(i,3))$, 四个元素均为字节。则 $ck(i,j) = (4i+j) \times 7 \pmod{256}$ 。32个固定参数 CK_i 详见GB/T 32907-2016《信息安全技术 SM4分组密码算法》。

部分媒体新闻链接:

全国信息安全标准化技术委员会: <https://www.tc260.org.cn/front/postDetail.html?id=20210628121559>

密码君: <https://mp.weixin.qq.com/s/8TyZT-d4r0gXu0J9AgubPw>

国家密码管理局: https://www.oscca.gov.cn/sca/xwdt/2021-07/08/content_1060866.shtml

搜狐网: https://www.sohu.com/a/474836321_121124361

网易: <https://www.163.com/dy/article/GDM8RVEP0538JG0V.html>

南网首个“云巢”搭建成功 WAPI应用到无人机作业领域 保障数据安全传输

科技日报 南方电网报 中国电力新闻网



记者从广东电网公司机巡中心获悉，6月底，基于自主可控安全标准的无线WAPI网络技术，南方电网公司首个无人机作业“云巢”模块在广东云浮罗定调试成功，彻底解决无人机巡视数据传输的“最后一公里”难题。

“云巢相当于虚拟机巢，不需要机巢的实体硬件，通过软件即可实现和机巢类似的功能，实现无人机的任务远程下达、视频直播、照片自动回传等功能。”广东电网公司机巡管理中心技术应用推广部经理刘高介绍，基于“三维航线系统+WAPI无线网络”，云巢系统与无人机实现

指令交互，无人机接到指令后，在变电站或供电所大楼就能实现“不出门、不开车”作业，巡视画面实时传输到内网直播，全程无需建设额外的无人机机巢硬件。

WAPI技术不仅确保终端的接入安全，提升电网安全运行水平，同时大幅减轻基层班组的工作负担，通过“云巢”系统，无人机在完成自动巡检作业后，可直接连接WAPI无线网络，实现原始影像数据的安全快速传输，有效解决了数据传输量大、速度慢、繁琐耗时等问题。

在办公区域部署WAPI网络，是打通无人机数据上传“最后一公里”最安全、最快捷的技术路径。WAPI网络在无人机领域的应用，有力支撑了地市局、县区局输配电数字化转型，为无人机智能巡检提供可靠、高速、优质的通信网络。同时，该功能还可用于应急救援、线路快速通道巡检、精细化巡检、输变配电的一体化巡检等作业场景。

部分媒体新闻链接：

科技日报/中国科技网：http://www.stdaily.com/index/kejixinwen/2021-07/15/content_1178888.shtml

南方电网报：<http://www.chinapower.com.cn/dww/jscx/20210716/88707.html>

中华网：<https://tech.china.com/article/20210716/20210716828456.html>

中国电力新闻网：http://www.cpn.cn/news/nyqy/202107/t20210719_1406591.html

中国高新网：<http://www.chinahightech.com/html/chaopin/xjs/2021/0716/5600614.html>

《党委（党组）网络安全工作责任制实施办法》解读

关键基础设施安全应急响应中心

一、前言

2021年8月4日,《人民日报》头版发布《中国共产党党内法规体系》一文。同时,《中国共产党党内法规汇编》公开发布,收录了《党委（党组）网络安全工作责任制实施办法》(以下简称《实施办法》),正式揭开了《实施办法》的神秘面纱。党内法规具有强烈政治属性、鲜明价值导向、科学治理逻辑、统一规范功能,高度凝结党的理论创新和实践经验,是党的中央组织,中央纪律检查委员会以及党中央工作机关和省、自治区、直辖市党委制定的体现党的统一意志、规范党的领导和党的建设活动、依靠党的纪律保证实施的专门规章制度。《实施办法》作为《中国共产党党内法规体系》唯一收录的网络安全领域的党内法规,它的公开发布将对厘清网络安全责任、落实保障措施、推动网信事业发展产生巨大影响。本文将从责任主体、责任范围、责任事项、问责主体、启动问责的条件、问责措施等角度切入,深入解读这份首次面世的网络安全党内法规。

二、责任主体

(一) 什么是党委、党组

《实施办法》第一条明确指出,本办法是为了明确和落实党委（党组）领导班子、领导干部的网络安全责任。为了理解《实施办法》,首先要弄清什么是党委和党组。1.党组。《党章》第四十八条规定,在中央和地方国家机关、人民团体、经济组织、文化组织和其他非党组织的领导机关中,可以成立党组。《中国共产党党组工作条例》规定,党组是党在中央和地方国家机关、人民团体、经济组织、文化组织和其他非党组织的领导机关中设立的领导机构,在本单位发挥领导作用,是党对非党组织实施领导的重要组织形式。常见的党组有:国务院党组,国务院某部门党组,某省政府机关党组、人大常委会机关党组、政协机关党组、法院党组、检察院党组,中管企业党组,工会、妇联等人民团体党组等。2.党委。《党章》第十条规定,党的最高领导机关,是党的全国代表大会和它所产生的中央委员会。党的地方各级领导机关,是党的地方各级代表大会和它们所产生的委员会。党的各级委员会向同级的代表大会负责并报告工作。3.党委与党组的主要区别。一是产生方式不同,党委由同级党的代表大会选举产生,党组由批准其设立的党组织批准成立。二是负责对象不同,党委向选举其产生的党的代表大会负责,党组则必须服从批准其设立的党组织领导。三是设立权限不同,党中央或本级地方党委可以审批设立党组,而党组不得审批设立党组。尽管有以上的不同之处,党委与党组还具有一个最重要的共同特点,即在本单位本组织的范围内,发挥领导核心作用。《党章》第四十八条规定:“党组发挥领导核心作用。党组的任务,主要是负责贯彻执行党的路线、方针、政策;加强对本单位党的建设的领导,履行全面从严治党责任;讨论和决定本单位的重大问题;做好干部管理工作;讨论和决定基层党组织设置调整和发展党员、处分党员等重要事项;团结党外干部和群众,完成党和国家交给的任务;领导机关和直属单位党组织的工作。”(二) 各级党委（党组）、各级（各地区各部门）网络安全和信息化领导机构、行业主管监管部门《实施办法》规定,具有网络安全工作责任的主要有三类主体:各级党委（党组）、各地区各部门网络安全和信息化领导机构、行业主管监管部门。1.各级党委（党组）。各地区各部门各级党政机关、关键信息基础设施

运营单位、重要数据和个人信息处理者等单位的党委（党组）是网络安全工作的责任主体。《实施办法》第二条规定：“按照谁主管谁负责、属地管理的原则，各级党委（党组）对本地区本部门网络安全工作负主体责任，领导班子主要负责人是第一责任人，主管网络安全的领导班子成员是直接责任人。”此条规定明确了从中央到地方和基层的政府机关、企事业单位、人民团体中各级党委和党组，是网络安全工作的责任主体，并且进一步明确了领导班子主要负责人和相关领导班子成员的责任。2.各级（各地区各部门）网络安全和信息化领导机构。《实施办法》第五条、第六条分别规定，各级（各地区各部门）网络安全和信息化领导机构具有分析研判网络安全信息、统筹协调网络安全检查、组织通报网络安全信息等职责。3.行业主管监管部门。《实施办法》第四条规定：“行业主管监管部门对本行业本领域的网络安全负指导监管责任。没有主管监管部门的，由所在地区负指导监管责任。”

三、责任范围

《实施办法》所划定的责任主体，具有各自不尽相同的责任范围，形成一张相互交织、没有死角的网络安全责任网络，严密覆盖每一个行业和领域、地区、关键信息基础设施运营单位、党政机关。

（一）行业和领域。按照《实施办法》第四条，本行业本领域的网络安全检查、事件处置，由主管监管部门负责指导监管。没有主管监管部门的行业，由所在地区负指导监管责任。电信、能源、金融等行业的网络安全工作，由相关主管监管部门负责；少数没有主管监管部门的行业、领域，由所在地区网信领导机构负责。（二）地区。按照《实施办法》第五条，本地区的网络安全事件汇集、分析研判、组织指导信息通报、统筹协调网络安全检查等工作，由本地区的网信领导机构负责。（三）关键信息基础设施运营单位。关键信息基础设施运营单位网络安全工作，由本单位的党委（党组）负主体责任，由相关行业主管监管部门负指导监管责任，没有主管监管部门的关基单位，由所在地区网信领导机构负指导监管责任。（四）党政机关。按照《实施办法》第三条，党政机关本单位的网络安全工作，由本单位党委（党组）负主体责任。另外，《实施办法》第四条还对可能出现的交叉重叠责任进行了划分协调：“各地区开展网络安全检查、处置网络安全事件时，涉及重要行业的，应当会同相关主管监管部门进行。”

四、责任事项

《实施办法》划定的不同的责任主体，具有不同的责任事项。

（一）各级党委（党组）按照《实施办法》第三条，各级党委（党组）主要承担的网络安全责任是：1.认真贯彻落实党中央和习近平总书记关于网络安全工作的重要指示精神 and 决策部署，贯彻落实网络安全法律法规，明确本地区本部门网络安全的主要目标、基本要求、工作任务、保护措施；2.建立和落实网络安全责任制，把网络安全工作纳入重要议事日程，明确工作机构，加大人力、财力、物力的支持和保障力度；3.统一组织领导本地区本部门网络安全保护和重大事件处置工作，研究解决重要问题；4.采取有效措施，为公安机关、国家安全机关依法维护国家安全、侦查犯罪以及防范、调查恐怖活动提供支持和保障；5.组织开展经常性网络安全宣传教育，采取多种方式培养网络安全人才，支持网络安全技术产业发展。（二）行业主管监管部门《实施办法》第四条规定：行业主管监管部门对本行业本领域的网络安全负指导监管责任。没有主管监管部门的，由所在地区负指导监管责任。主管监管部门应当依法开展网络安全检查、处置网络安全事件，并及时将情况通报网

络和信息系统所在地区网络安全和信息化领导机构。各地区开展网络安全检查、处置网络安全事件时，涉及重要行业的，应当会同相关主管监管部门进行。（三）各级（各地区各部门）网络安全和信息化领导机构《实施办法》第五条：各级网络安全和信息化领导机构应当加强和规范本地区本部门网络安全信息汇集、分析和研判工作，要求有关单位和机构及时报告网络安全信息，组织指导网络安全通报机构开展网络安全信息通报，统筹协调开展网络安全检查。《实施办法》第六条：各地区各部门网络安全和信息化领导机构应当向中央网络安全和信息化委员会及时报告网络安全重大事项，包括出台涉及网络安全的重要政策和制度措施等。各地区各部门网络安全和信息化领导机构每年向中央网络安全和信息化委员会报告网络安全工作情况。

五、启动问责的条件

《实施办法》第八条规定了两种启动问责的条件，一是按行为，二是按后果。

（一）按行为问责《实施办法》第八条第一款规定：各级党委（党组）违反或者未能正确履行本办法所列职责，按照有关规定追究其相关责任。按此规定，责任主体若未履行本办法所列职责，有违反本办法的不作为或乱作为行为，则按有关规定追究相关责任。（二）按后果问责《实施办法》第八条第二款规定：“有下列情形之一的，各级党委（党组）应当逐级倒查，追究当事人、网络安全负责人直至主要负责人责任。协调监管不力的，还应当追究综合协调或监管部门负责人责任。1.党政机关门户网站、重点新闻网站、大型网络平台被攻击篡改，导致反动言论或者谣言等违法有害信息大面积扩散，且没有及时报告和组织处置的；2.地市级以上党政门户网站或者重点新闻网站受到攻击后没有及时组织处置，且瘫痪6小时以上的；3.发生国家秘密泄露、大面积个人信息泄露或者大量地理、人口、资源等国家基础数据泄露的；4.关键信息基础设施遭受网络攻击，没有及时处置导致大面积影响人民群众工作、生活，或者造成重大经济损失，或者造成严重不良社会影响的；5.封锁、瞒报网络安全事件情况，拒不配合有关部门依法开展调查、处置工作，或者对有关部门通报的问题和风险隐患不及时整改并造成严重后果的；6.阻碍公安机关、国家安全机关依法维护国家安全、侦查犯罪以及防范、调查恐怖活动，或者拒不提供支持和保障的；7.发生其他严重危害网络安全行为的。”

六、问责主体

《中国共产党问责条例》第十二条规定：“问责决定应当由有管理权限的党组织作出”。《实施办法》第九条规定了实施问责的主体：“对领导班子、领导干部进行问责，应当由有管理权限的党组织依据有关规定实施。”回答“谁来实施问责”这个问题的关键，在于准确理解“有管理权限的党组织”。

按照党的民主集中制原则，下级党组织服从上级党组织，“有管理权限的党组织”即为被问责对象的上级党组织。然而，在党的组织结构中，普遍存在双重领导或多重领导的情形。另外，因为存在分管领域的划分，党组织之间还存在归口领导管理、归口指导、协调或监督职责等关系。如高校党组织，往往同时受地方党组织、教育部门党组织的双重领导；国有企业，往往受国资监管部门的领导，同时受所在行业主管部门的指导。对此，为了准确理解“有管理权限的党组织”，可参考《中国共产党重大事项请示报告条例》的规定。

《条例》第二章“党组织请示报告主体”对于党组织向上请示的对象做出规定，一是在双重领导的情况下，向负有主要领导职责的上级党组织请示报告，二是在归口领导、管理的情况下，服从批准其设立的党组织的领导。据此，将“有管理权限的党组织”理解为被问责党组织的上级党组织，或批准其设立的党组织则更为准

确。需要说明的是，虽然各级网信办有可能不是被问责对象的上级党组织，但作为网信领域发挥党的领导作用的核心机构，各级网信部门在实施问责中起到重要作用。《实施办法》第九条第二款规定：“各级网络安全和信息化领导机构办公室可以向实施问责的党委(党组)、纪委(纪检组)提出问责建议。”

七、问责措施

《实施办法》第九条规定：“对领导班子、领导干部进行问责，应当由有管理权限的党组织依据有关规定实施。”此处的“有关规定”，即为《中国共产党问责条例》。《中国共产党问责条例》第八条规定了三种针对党组织的问责方式，即检查、通报、改组；四种针对党的领导干部的问责方式，即通报、诫勉、组织调整或者组织处理、纪律处分。给予纪律处分的，依照《中国共产党纪律处分条例》追究纪律责任。

八、保障措施

(一) 表彰奖励

《实施办法》第七条规定，用表彰奖励的形式促进网络安全工作的落实：“中央网络安全和信息化委员会办公室会同有关部门按照国家有关规定对网络安全先进集体予以表彰，对网络安全先进工作者予以表彰奖励”。2016年，中央网信办、教育部指导中国互联网发展基金会网络安全专项基金设立“网络安全人才奖”、“网络安全优秀教师奖”等，在当年的国家网络安全宣传周上，对19名网络安全杰出人才、优秀人才及优秀教师进行表彰。自此，中央网信办每年都组织开展相关表彰活动。

(二) 干部考核《实施办法》第十条规定：“各级党委(党组)应当建立网络安全责任制检查考核制度，完善健全考核机制，明确考核内容、方法、程序，考核结果送干部主管部门，作为对领导班子和有关领导干部综合考核评价的重要内容”。

(三) 审计保障《实施办法》第十一条规定：“各级审计机关在有关部门和单位的审计中，应当将网络安全建设和绩效纳入审计范围”。

浅谈我国商用密码标准体系

密码君

一、《密码法》关于商用密码标准体系的规定

《密码法》第二十二条规定：国家建立和完善商用密码标准体系。国务院标准化行政主管部门和国家密码管理部门依据各自职责，组织制定商用密码国家标准、行业标准。国家支持社会团体、企业利用自主创新技术制定高于国家标准、行业标准相关技术要求的商用密码团体标准、企业标准。

商用密码标准化是实现商用密码技术自主创新、促进商用密码产业发展、构建商用密码应用体系的重要支撑。《密码法》明确商用密码标准体系包括商用密码国家标准、行业标准、团体标准和企业标准。商用密码国家标准、行业标准属于政府主导制定的标准，商用密码团体标准、企业标准属于市场主体自主制定的标准。商用密码国家标准由国家标准化管理委员会组织制定，代号为GB。商用密码行业标准由国家密码管理局组织制定，报国家标准化管理委员会备案，代号为GM。商用密码团体标准由商用密码领域的学会、协会等社会团体制定，商用密码企业标准由商用密码企业制定或者企业联合制定。

二、密码行业标准化技术委员会是我国密码行业唯一标准化组织

2011年10月，经国家标准化管理委员会批准，国家密码管理局设立了密码行业标准化技术委员会。密码行业标准化技术委员会作为我国密码行业唯一标准化组织，受国家密码管理局委托，主要职责包括：(1)提出密码行业标准规划和年度标准制定、修订计划的建议；(2)组织密码行业标准的编写、审查、复审等工作；(3)组织密码领域的国家和行业标准的宣传贯彻，推荐密码领域标准化成果申报科技进步奖励，或向国家标准化管理委员会提出项目奖励建议；(4)受国家标准化管理委员会委托，对相关国际标准文件进行表决、审查我国提案，并组织开展国际技术交流与合作等。

三、我国商用密码标准体系建设情况

截至2019年12月，国家标准化管理委员会已发布商用密码国家标准29项，国家密码管理局已发布商用密码行业标准91项，覆盖商用密码技术、产品、服务、应用、检测和管理等多个领域，构建了较为齐全完备的商用密码标准体系，有效发挥了商用密码标准在引领科技进步、推动产业发展、促进互联互通、助力应用推进、优化管理服务等方面的重要作用。

四、商用密码行业标准的分类

当前，商用密码的行业标准分为基础类标准、应用类标准、检测类标准和管理类标准。基础类标准为其他三类标准提供了底层、共性支撑（如术语、算法、协议、产品等）；检测类标准为其他三类标准和应用类标准提供了合法性检测的功能，保障商用密码使用的合法性；管理类标准为其他三类标准提供了管理功能；应用类标准为上层具体的密码产品、服务应用提供支持。

五、关于商用密码强制性国家标准和推荐性国家标准、行业标准

我国标准按照实施效力分为强制性标准和推荐性标准。强制性标准仅有国家标准一级。推荐性标准包括推荐性国家标准和行业标准。也就是说,商用密码行业标准都是推荐性标准。

强制性标准必须执行,不符合强制性标准的产品、服务,不得生产、销售、进口或者提供。违反强制性标准的,依法承担相应的法律责任。

国家鼓励采用推荐性标准,即从业单位自愿采用推荐性标准。同时国家还会采取一些正向激励措施,鼓励企业采用推荐性标准。但在有些情况下,推荐性标准的效力会发生转化,必须执行,例如:

(1)推荐性标准被相关法律、法规、规章等引用,则该推荐性标准具有相应的强制约束力,应当按照法律、法规、规章的相关规定予以实施。

(2)推荐性标准被企业进行了自我声明公开的,企业必须执行该推荐性标准。企业生产的产品与明示标准不一致的,根据《产品质量法》等法律法规承担相应的法律责任。

(3)推荐性标准被合同双方作为产品或服务交付的质量依据的,该推荐性标准对合同双方具有约束力,双方必须执行该推荐性标准,并依据《合同法》的规定承担法律责任。

六、商用密码标准的法律效力

《密码法》第二十四条规定:商用密码从业单位开展商用密码活动,应当符合有关法律、行政法规、商用密码强制性国家标准以及该从业单位公开标准的技术要求。国家鼓励商用密码从业单位采用商用密码推荐性国家标准、行业标准,提升商用密码的防护能力,维护用户的合法权益。商用密码从业单位开展商用密码活动应当依照有关法律、行政法规的规定行使权利和履行义务,是遵守法律的必然要求。商用密码从业单位开展商用密码活动,除了遵守法律、行政法规,还应当符合商用密码强制性国家标准以及该从业单位公开标准的技术要求。此外,国家鼓励商用密码从业单位采用商用密码推荐性国家标准、行业标准。

七、我国商用密码国际标准化开展情况

《密码法》第二十三条第一款规定:国家推动参与商用密码国际标准化活动,参与制定商用密码国际标准,推进商用密码中国标准与国外标准之间的转化运用。我国高度重视商用密码国际标准化工作,大力推进以我国自主设计研制的SM系列密码算法为代表的中国商用密码标准纳入国际标准,积极参与国际标准化活动,加强国际交流合作。2011年9月,我国设计的祖冲之(ZUC)算法纳入国际第三代合作伙伴计划组织(3GPP)的4G移动通信标准,用于移动通信系统空中传输信道的信息加密和完整性保护,这是我国密码算法首次成为国际标准。2015年5月起,我国陆续向ISO提出了将SM2、SM3、SM4和SM9算法纳入国际标准的提案。2017年,SM2和SM9算法正式成为ISO/IEC国际标准。2018年,SM3算法正式成为ISO/IEC国际标准。2020年4月,ZUC序列密码算法正式成为ISO/IEC国际标准。① 2021年2月,SM9算法正式成为ISO/IEC国际标准。② 2021年6月,SM4算法正式成为ISO/IEC国际标准。③(①②③为小编补充添加)我国商用密码国际标准体系已初步成型,为密码在全球范围的发展与应用提供了中国方案,贡献了中国智慧。在转化运用国际标准方面,商用密码行业标准GM/T0028《密码模块安全技术要求》和GM/T0039《密码模块安全检测要求》,分别参考国际标准ISO19790和

ISO24759编制，为规范商用密码产品管理、提升商用密码产品安全防护能力发挥了重要作用，充分体现了商用密码标准制定的开放性。

八、鼓励企业、社会团体和教育、科研机构等参与商用密码国际标准化活动

《密码法》第二十三条第二款规定：国家鼓励企业、社会团体和教育、科研机构等参与商用密码国际标准化活动。企业、社会团体和教育、科研机构等全面深入地参与商用密码国际标准的制修订等国际化活动，是全球化的必然趋势和要求，有利于提升商用密码技术的全球影响力，同时也为降低包括密码脆弱性在内的全球网络安全整体风险贡献中国智慧和提供中国方案。

九、关于商用密码从业单位公开标准的技术要求和作用

《密码法》规定了企业标准自我声明公开和监督制度,调整的对象是企业生产的产品和提供的服务所执行的标准，这类标准规定了企业生产的产品和提供的服务所应达到的各类技术指标和要求，是企业对其产品和服务质量的硬承诺，应当公开并接受市场监督。企业生产的商用密码产品和提供的商用密码服务，如果执行国家标准、行业标准和团体标准，企业应该公开相应的标准名称和标准编号；如果企业生产的产品和提供的服务所执行的标准是本企业制定的企业标准，企业除了公开相应的标准名称和标准编号，还应当公开企业产品、服务的技术指标。公开指标的类别和内容由企业根据自身特点自主确定,企业应对公开的产品和服务标准的真实性、准确性、合法性负责。企业生产的产品和提供的服务应当符合企业自我声明公开标准提出的技术要求，不符合企业自我声明公开标准提出的技术要求的，应依法承担相应的责任。

联盟人谈标准创新系列（三）

【编者按】 WAPI产业联盟是国内首家专注于网络安全且目前最具规模的产业联盟，是国家科技部首批A类产业技术创新战略联盟和国家标准委首批团体标准试点单位。15年间，联盟在推动技术产业创新和成果转化、服务市场用户和产业链需求、促进行业可持续发展等方面，开展了很多务实工作，在标准创制与实施上成果显著。2015-2017年期间，联盟承接了国家标准委委托的首批国家团体标准试点工作，当时全国入选的联盟仅有7家。其中的重要工作之一就是通过试点工作，完成国家在技术创新和团体标准方面的发展规划。

截至2021年6月，WAPI产业联盟已组织开展了170余项标准的制修订，为构建最基础最共性的网络安全架构体系提供有效支撑，其中发布（获发布）国际标准（ISO/IEC）14项、欧洲标准3项，国家标准41项，国家军用标准4项，行业标准7项，团体标准68项。基于TePA安全架构形成的14项国际标准，为我国在物联网、有线以太网、无线个域网、电子标签、同轴双向网络、传感器网络、有线局域网、无线城域网、未来网络、磁域网络等等众多领域形成了标准国际化超前布局，为解决网络安全“卡脖子”问题做出有力支撑。

今年“十四五”规划纲要全文35处40次提及标准化工作，联盟社会组织正在成为组织和开展高质量标准化工作的重要力量。因此，《在路上》开辟“联盟人谈标准创新系列”专栏，分享WAPI产业联盟秘书处专职化工作人员在标准化方面的实践与思考，也希望藉此和业界同仁多多交流。

本系列文章的版权为原作者本人所有，转载或者引用本文内容请注明来源及原作者。

刘 婷：标准领航，助力关键信息基础设施安全防护建设

WAPI产业联盟 刘 婷

摘 要：随着信息技术的发展，关键信息基础设施（以下简称“关基”）正全方位地进入信息化、数字化、网络化，为各行业的创新发展带来新动能。无线局域网（WLAN）是无线高速数据通信的主流技术，具有带宽高、成本低、部署方便等特点，也因此成为许多行业“关基”实施“最后一公里”无线接入业务的理想选择。然而在当前的网络安全态势下，针对“关基”的攻击手段层出不穷，网络安全事件时有发生，对于缺乏物理防护（线路）的无线网络来说就更多了一层危险。因此，如何在利用WLAN部署优势的同时确保安全，继而满足“关基”的业务运行需求，一直是政府管理机构、行业主管部门以及市场用户重点关注的问题。

本文作者基于多年在无线网络和网络安全领域的标准化工作实践，从技术、产业、市场方面，全面论证了具有我国自主知识产权的WAPI是“关基”建设安全无线局域网的最佳选择，同时揭示了标准在“关基”实

际运行和管理中发挥的重要作用，对各行业“关基”制定无线网络技术路线，以及规划、设计、部署和应用WLAN业务具有实际的参考意义。

关键词：关键信息基础设施，安全，无线局域网，WAPI，标准

1 引言

关键信息基础设施，指的是面向公众提供网络信息服务或支撑能源、通信、金融、交通、公共事业等重要行业运行的信息系统或工业控制系统。“关基”作为经济社会运行的神经中枢，承载着大量国家和行业基础数据、重要政务数据及公民个人信息，其安全防护问题直接影响我国数字经济发展和网络强国建设。^[1]随着信息技术的发展，“关基”正全方位地进入信息化、数字化、网络化，为各行业的创新发展带来新动能。近年来，随着《网络安全法》、《密码法》、等级保护2.0国家标准的相继出台，从国家到各行业对于“关基”的网络安全性以及合法合规性都做出了明确部署和具体要求。

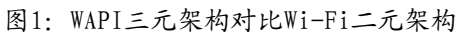
无线局域网（以下简称“WLAN”）是无线高速数据通信的主流技术，相较于另一主流技术4G/5G，具有带宽高、成本低、部署方便等特点。WLAN作为有线网络的延伸，可在局部区域（约100米）内为用户提供高达9.6Gbps的高速率数据通信服务，也因此成为了许多行业“关基”实施“最后一公里”无线接入业务的理想选择。然而在当前的网络安全态势下，针对关键信息基础设施的攻击手段层出不穷，网络安全事件时有发生，对于缺乏物理防护（线路）的无线网络来说就更多了一层危险。因此，如何在利用WLAN部署优势的同时确保安全，继而满足“关基”的业务运行需求，一直是政府管理机构、行业主管部门以及市场用户重点关注的问题。

2 自主可控的WAPI技术标准，能为“关基”WLAN建设提供强有力的安全保障

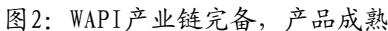
（一）WAPI技术优势显著，是迄今全球WLAN唯一安全的机制，Wi-Fi存在大量安全缺陷

WLAN技术在全球范围内发展至今20多年，目前标准体系方面已相对统一，但在安全机制部分有两条路线：一个是美国主导的Wi-Fi安全技术802.11i，另一个是采用了国产密码技术的国家标准WAPI（无线局域网鉴别与保密基础架构）。因Wi-Fi在安全架构上存在重大缺陷，不法分子可以轻易地破解Wi-Fi密码，继而非法侵入网络，实施盗取数据、恶意攻击、植入木马等网络攻击活动。近年来，由Wi-Fi引发的网络安全事件频频被央视3.15晚会等大量媒体曝光，其网络和产品已被视为安全“灰犀牛”，成为了“关基”在无线网络建设中不敢涉足的禁区。

WAPI是采用了国产密码算法，具有我国自主知识产权的无线局域网安全协议技术，已在2006年被采纳并发布为GB 15629.11系列国家标准。WAPI创新性地采用三元对等安全架构（TePA），包含2个基础架构（身份鉴别WAI、数据保密WPI），通过五次传递流程实现了终端（STA）和无线接入点（AP）的对等双向鉴别，确保了合法用户接入合法网络，迄今未发现安全漏洞。



WAPI因其安全性及技术先进性，多年来一直受到国家的大力支持，包括设立专项、政策支持、成立WAPI产业联盟等，以更好地推动和落实产业化、服务市场应用需求。经过十余年努力和发展，WAPI已成为全球无线局域网芯片的标准配置，截至2021年6月，集成WAPI的芯片已达500多个型号，全球累计出货量已超过160亿颗，具备WAPI安全能力的无线局域网产品超过17000款，物联网领域的标准化接口和集成WAPI模组技术已非常成熟。WAPI产业联盟现有106家会员中，已包括三大电信运营商和有代表性的ICT领域企业，覆盖从芯片设计到整机、系统集成、测试等产业链各环节的骨干企业。^[2]目前，WAPI已广泛服务于政务、军队、公安、海关、能源、交通、医疗、教育等重要行业的关键信息基础设施，为其业务活动及数据资产安全提供技术支撑与保障。



（三）技术扩展性方面，TePA安全架构可广泛应用于各种“关基”网络形态

全球网络安全架构迄今共经历三代：二元架构、二转三元过渡架构、三元架构。GB 15629.11国家标准规范的WAPI所基于的TePA，实现了终端（用户）和无线接入点（网络）的对等双向鉴别，目前仍是第三代最稳定的架构，并已经被发布为ISO/IEC国际标准。

WAPI技术和RFID领域（TRAIS安全协议）、NFC（NEAU安全协议）、以太网（TLSec），以及我国自主IP层安全协议（TISec）均基于我国自主的三元对等安全架构，上述物联网相关安全协议均已是我国国家标准。随着“关基”数字化、网络化、智能化的深入推进，目前已出现一些新型业务和差异化的网络形态，如机器人巡检、可视化作业、移动巡检、数据采集等业务，这些业务网络具有大带宽、移动性、大连接等特点，涉及大量的物联网终端应用。基于相同的安全架构，将在网络的整体安全性、统一部署和管理等方面具备显著优势。

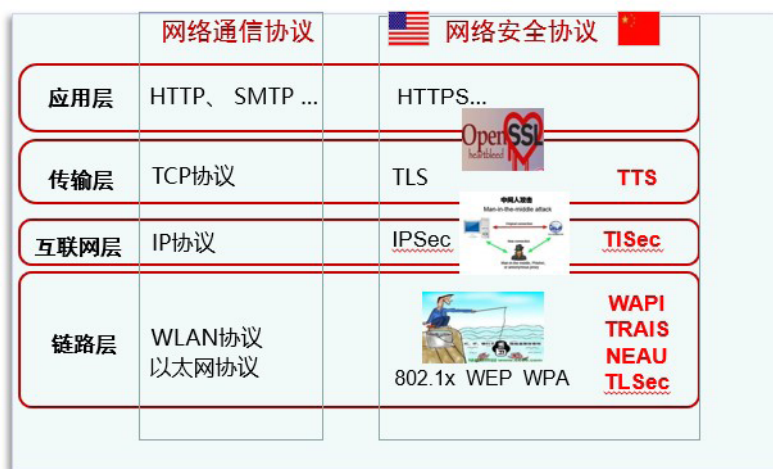


图3：三元对等架构TePA保障多业务通信安全

3 团体标准是国家/行业标准的有效补充，是快速满足“关基”WAPI业务及产品需求的“指南针”

（一）团体标准天然为“用”而生，聚焦产业技术共性关键问题，服务市场

团体标准是由具备相应能力社会组织或者产业联盟制定的标准，是以标准组织或联盟内部共识为基础。团体标准具有灵活性，即制定程序更加灵活，标准的立项、编写、批准等都可自行决定，因此制定及发布的速度要比其它类型标准快得多。团体标准具有先导性，即能够快速反映市场需求，继而通过标准的制定和发布反哺市场，推动产业和技术良性发展。^[3]

WAPI技术成为国家标准（GB 15926.11系列标准）后，随着产业化和市场应用的不断深入，标准体系中仅包含技术规范的局限性日益凸显：因缺少规范统一的安全测试评价方法和流程，使得检测机构对符合GB 15926.11系列技术标准的测试方法和结果不一致，直接导致流向市场的产品良莠不齐。在这种背景下，WAPI产业联盟积极组织其生产、用户、检测等成员单位，先后制定和发布了5项团体标准，构成了完善、科学、操作性强的WLAN测试团体标准体系，并在产业群体范围内先行应用。其中，T/WAPIA 002—2010《无线局域

网接入点技术要求与测试方法》、T/WAPIA 003—2010《无线局域网接入控制器技术要求与测试方法》、T/WAPIA 004—2010《无线局域网站点技术要求与测试方法》、T/WAPIA 005—2010《无线局域网鉴别服务器技术要求与测试方法》4项标准实施之后，取得了良好的效果，并因满足了国家发展WLAN的迫切需要，具有广泛推广和应用价值，已被转化为国家标准GB/T 32420—2015《无线局域网测试规范》并实施。

随着近年来各行业“关基”对安全无线局域网需求的日益旺盛，市场用户对WAPI检测又提出了更高更精细的要求。为进一步推进GB/T 32420—2015实施，WAPI产业联盟积极规划了《GB/T 32420实施指南》系列标准，在国家标准基础上进一步提升技术指标和测试方法，并于2019年发布了T/WAPIA 037.2—2019《GB/T 32420实施指南 第2部分：无线局域网设备测试》，目前，上述团体标准已成功服务于北京大兴国际机场、冬奥会、世界园艺博览会、北京边检等“关基”WLAN项目，为项目的按期优质建成提供了有效支撑，也推动了WAPI技术产业的高质量发展。

（二）团体标准可快速满足多样性需求，是实现各行业“关基”WAPI网络好用的有效手段

通信行业区别于其它行业的一个显著特点是，因涉及不同厂商、不同品牌产品之间的互联互通，因此必须标准先行，依照标准实施产品开发，才能保证产品质量和互联互通性。而另一方面，不同行业“关基”对WAPI业务的需求差异较大，涉及的网络设备、终端机具从物理形态到技术指标多种多样，因此对于一些共性关键技术，或者是对于一些产品的个性化、高标准需求，通过制定团体标准来定义和规范往往最为快速高效。

以两个行业“关基”WAPI项目建设为例：一个是北京大兴国际机场，其网络部署属于异构网络，构成网络的硬件和软件均来自不同厂商，基于网络所开展的业务形态各异，网络环境复杂。在这种环境下，对WAPI产品间的协议符合性、互联互通性、网络承载等能力要求非常高。为满足该项目实际建设需求，WAPI产业联盟针对大规模组网中的证书管理问题，制定并发布了T/WAPIA 038—2019《信息安全技术 终端实体证书管理》，标准主要包括了数字证书文件颁发的格式和证书文件下载机制，定义了安全的终端实体证书管理协议，能够统一对证书进行管理，将证书自动下载、更新等方面的技术细节标准化，指导证书在多种网络领域和异构网络环境下的应用实施。标准一经发布即迅速应用到机场项目的建设，在建设工期紧、施工难度大的情况下，顺利完成了WAPI网络的建设任务，为机场项目献礼国庆70周年贡献了力量。

另一个是2019年底开始建设的南方电网变电站项目，涉及五省全域，其WAPI项目建设需求一方面需要包括室内外无线信号全方位覆盖、视频监控终端无延时、无卡顿传输数据、单站接入多终端多、大带宽等无线通信指标要求，也需要结合变电站实际业务环境，符合电磁兼容、防雷击、防水防尘高低温等指标要求。为指导厂商高效研发并生产出符合电力行业需求的产品，WAPI产业联盟于2020年3月发布了TWAPI 040.2—2020《关键信息基础设施无线局域网技术要求 第2部分：电力行业扩展要求》。这项团体标准，是在之前制定的TWAPI 040.1—2020《关键信息基础设施无线局域网技术要求 第1部分：通用要求》的基础上，根据电力行业的技术指标、测试方法等进行分类规范形成的行业扩展要求，具有紧密贴合电力行业生产和管理特点、聚焦行业专业机具和高安全网络系统等特质，为保障电力行业“关基”产品质量、提升互联互通互操作能力提供了必要指引。



图4: “关基”团体标准体系

4 小结

推进关键信息基础设施建设，推动国家治理体系和治理能力现代化，离不开“标准”二字。WAPI作为迄今全球WLAN唯一安全的机制，目前已形成从技术指标到测试方法的一套完整的国家标准体系。就技术本身而言，因其具有“采用全球先进的三元对等安全架构、国产密码、技术扩展性强、产业化完备、市场应用经验丰富”等特点，同时符合《网络安全法》、《密码法》、等保2.0系列国家标准等法律法规，因而是保障我国以及各行各业“关基”无线局域网安全的最佳选择。在网络建设和运行的过程中，标准也是保障网络可用、好用的必要指引，除了基础性、通用性的国家标准之外，团体标准也发挥着重要作用，二者互为支撑，相辅相成，共同为各行业“关基”无线网络的高效运行保驾护航，也在应用中彰显标准旺盛的生命力和存在价值。

参考文献

- [1] 高原，吕欣，李阳，穆琳，韩晓露，鲍旭华.国家关键信息基础设施系统安全防护研究综述.信息安全研究[J]，2020(006),001.
- [2] WAPI产业联盟.WAPI标准产业应用及环境监测报告[R].2021(06).
- [3] 韩子燕，李键.团体标准维度探析及其实施条件——基于《中华人民共和国标准化法（修订草案）》的思考[J].标准科学.2017(000),007.

作者刘婷，系WAPI产业联盟公共事务总监，无线网络安全标准化委员会委员。

工信部：

就网络安全产业高质量发展三年行动计划（2021-2023年）征求意见

工业和信息化部7月12日面向社会就《网络安全产业高质量发展三年行动计划（2021-2023年）征求意见稿》公开征求意见。

《征求意见稿》重点包括：以推动网络安全产业高质量发展为目标，促进创新链、产业链、价值链的协同发展。加强基础性、通用性、前瞻性安全技术研究，加快关键核心技术攻关。提升大数据、人工智能、密码技术在安全领域的应用水平。推动网络安全架构向内生、自适应发展，加快开展基于开发安全运营、主动免疫、零信任等框架的网络安全体系研发。强化基础网络安全理论研究，促进研究成果应用转化，提升网络安全领域关键核心技术创新能力。充分发挥网络安全相关行业企业联盟、协会作用，通过技术攻关、项目合作、人才培养、园区建设等多种形式，促进创新要素流动，整合技术优势和资源优势，激发创新活力等。

网信办：

数字中国建设要统筹发展与安全

国家互联网信息办公室在2021年7月发布的《数字中国发展报告（2020年）》中提出，2021年数字中国建设要加快信息基础设施优化升级，加快交通、能源、市政、邮政等传统基础设施的数字化、智能化升级；统筹数据开发利用、隐私保护和公共安全，加快建立数据资源产权、交易流通、跨境传输和安全保护等基础制度和标准规范；加强信息技术专利创新，强化知识产权保护；加快培育信息技术产业生态，支持网信企业发展壮大，推动数字技术成果转化应用，打造具有国际竞争力的数字产业集群；打造一体化智慧化公共安全体系，支撑城市公共安全防控体系关口前移、精细管理和综合决策；鼓励社会力量参与“互联网+公共服务”，创新服务模式和产品；建立和完善数字技术应用审查机制和监管法律体系，开展算法规制、标准制定、安全评估等工作；鼓励企业、高校、科研机构、社会组织等开展国际科技合作，积极参与数字领域国际标准研究制定等。

网信办：

就《网络安全审查办法(修订草案)》征求意见

国家互联网信息办公室7月10日面向社会就《网络安全审查办法(修订草案征求意见稿)》公开征求意见。

《草案》重点包括：网络安全审查重点评估采购网络产品和服务活动、数据处理活动以及国外上市可能带来的国家安全风险，主要考虑产品和服务使用后带来的关键信息基础设施被非法控制、遭受干扰或破坏的风险；产品和服务供应中断对关键信息基础设施业务连续性的危害；产品和服务的安全性、开放性、透明性、来源的多样性，供应渠道的可靠性以及因为政治、外交、贸易等因素导致供应中断的风险；产品和服务提供者遵守中国法律、行政法规、部门规章情况；核心数据、重要数据或大量个人信息被窃取、泄露、毁损以及非法利用或出境的风险；国外上市后关键信息基础设施，核心数据、重要数据或大量个人信息被国外政府影响、控制、恶意利用的风险；其他可能危害关键信息基础设施安全和国家数据安全的因素等。

此外，本次修订还重点关注数据安全问题，并将刚刚通过的《数据安全法》纳入了修订依据。

肖亚庆：

大力发展网络安全产业将有效推动数字经济高质量发展

工业和信息化部党组书记、部长肖亚庆7月16日在《学习时报》发表的署名文章中指出，我国工业和信
息化发展面临的形势严峻复杂，做大做强数字经济意义重大而深远，应抓紧突破网络发展的前沿技术和具有国际竞争力的关键核心技术，构建安全可控的信息技术体系。要认真贯彻“十四五”规划纲要关于“推进产业数字化转型”的部署，加快产业结构优化升级。打造自主可控的标准体系，完善标准和服务体系，加快构建关键信息基础设施安全保障体系，强化网络安全保障。加强关键信息通信基础设施安全保障能力建设，推动网络安全产业创新发展，构建先进完备的网络安全产品体系，深化开展网络安全技术应用试点示范。

田世宏：

务实推进网络安全标准化工作高质量发展

国家市场监督管理总局副局长、国家标准化管理委员会主任田世宏在5月10日全国网络安全标准周中指出，网络安全标准化工作对于国家网络安全战略全局、国际竞争、产业创新发展以及民生保障具有重大意义。近年来网络安全标准化工作在顶层设计、标准体系、标准效能、国际标准化方面成效显著。下一步要加强标准体系规划布局，支撑网络安全重点工作和数字经济发展；要把握国际国内两个大局，持续提升我国网络安全领域国际话语权和影响力；要营造良好氛围，完善网络安全标准化工作支撑体系。

赵泽良：

网络安全标准要服务国家发展战略大局

中央网信办副主任、国家网信办副主任、信安标委主任委员赵泽良在5月10日全国网络安全标准周致辞中指出，国家网络安全标准化工作要以习近平总书记关于网络强国的重要思想为指导，着眼信息技术发展趋势，服务国家发展战略大局。一是站在新时代背景下，瞄准数字中国建设和促进数字经济发展的战略目标，积极推动网络安全标准与平台经济规则的融合促进，规范数据要素流通发展，引导平台经济安全健康发展；二是以国家网络安全法律体系建设为依据，不断完善网络安全标准与法律法规的配套衔接，围绕《网络安全法》和正在制定的《数据安全法》《个人信息保护法》开展标准化需求分析以及新技术新应用领域标准的前瞻性研究，为网络安全法律落地实施做好准备；三是突出标准规范性、引领性和实用性，提高标准质量和标准化工作水平，特别是要发挥网络安全标准在提升信息化驾驭能力和网络安全保障能力等方面的引领性作用。

谢永泉：

全面贯彻落实《密码法》 依法推进商用密码创新发展

国家密码管理局商密办副主任谢永泉在5月11日密码与信创产业创新峰会上指出，《密码法》的出台，对全面提升我国密码工作的规范化、科学化、法治化水平，维护我国网络空间安全、促进信息化发展具有里程碑意义。《密码法》规定了密码概念，明确了党管密码的根本原则，重塑了商用密码的管理体制机制。肯定了商用密码在维护国家网络安全中发挥的突出作用。

谢永泉指出，要建立完善的法规制度体系，强化原始创新，建设高质量标准体系，持续增强密码国家标准、行业标准供给质量，完善支持体制机制；要加快商用密码领域社会团体发展，强化密码应用安全性评估和管理，深入推进商用密码应用；要健全商用密码检测认证机制，完善商用密码检测认证体系，推进商用密码国际化发展。



联盟秘书处组织收看

庆祝中国共产党成立100周年大会盛况现场直播

WAPI产业联盟 周 园



2021年7月1日8时，庆祝中国共产党成立100周年大会在北京天安门广场隆重举行。中共中央总书记、国家主席、中央军委主席习近平发表重要讲话。联盟秘书处组织全体在京工作人员集中收看大会盛况现场直播，第一时间学习领会习近平总书记重要讲话精神。

“我们实现了第一个百年奋斗目标，在中华大地上全面建成了小康社会。”“中华民族迎来了从站起来、富起来到强起来的伟大飞跃，实现中华民族伟大复兴进入了不可逆转的历史进程！”习近平代表党和人民作出的庄严宣告，慷慨激昂，振奋人心。百年风华，再启新程。

秘书处同志们一致认为，庆祝大会庄重热烈，气势恢宏，震撼人心，催人奋进。习近平总书记的重要讲话，庄严宣告了我们党第一个百年奋斗目标如期实现，深刻阐述了中国共产党成立的伟大意义和伟大建党精神，深刻总结了建党一百年来我们党团结带领全国各族人民走过的光辉历程、取得的辉煌成就，深情展望了第二个百年奋斗目标和中华民族伟大复兴的光明前景，围绕以史为鉴、开创未来作出重大部署，并

向全体共产党员发出号召。习近平总书记的重要讲话高瞻远瞩，思想深邃，视野宏阔，内涵丰富，具有极强的思想性、政治性、理论性、指导性，是我们党在新的征程上更加坚定、更加自觉地牢记初心使命、开创美好未来的奋斗宣言，是指引新时代中国特色社会主义伟大事业的纲领性文献，通篇闪耀着马克思主义的光芒。

秘书处同志们纷纷表示，能共同见证这一伟大的历史时刻，我们感到无比喜悦和自豪。联盟秘书长张璐璐要求大家，要深入学习领会习近平总书记重要讲话的重大意义、科学内涵、精神实质和实践要求，切实用讲话精神武装头脑、指导实践、推动发展。更为重要的是，要结合习总书记重要讲话精神，牢记WAPI产业联盟的初心使命，坚定理想信念，践行党的宗旨，汲取建党百年奋斗的智慧 and 力量，在新的历史起点上做好网络安全创新联合体的本职工作。

2021年，WAPI产业联盟已组织并开展了庆祝中国共产党成立100周年系列庆祝活动，包括青山绿水义务植树、参观WAPI服务自主可控新基建示范项目、系统深入地学习中国共产党党史等等。



联盟秘书处系统学习中国共产党党史

WAPI产业联盟 周 园

今天我们将回顾第一个历史时期：开天辟地 中国共产党在新民主主义革命时期完成救国大业
(1921年7月-1949年10月)



今天我们将回顾第二个历史时期：改天换地 中国共产党在社会主义革命和建设时期完成兴国大业
(1949年10月-1978年12月)



WAPI产业联盟自2006年成立以来，始终坚决拥护中国共产党的领导，坚持以党的政治路线、中心工作和方针政策指导联盟日常工作。习近平总书记指出：“历史是最好的教科书。对我们共产党人来说，中国革命历史是最好的营养剂。多重温我们党领导人民进行革命的伟大历史，心中就会增加很多正能量。”

自2020年起，联盟秘书处的重要思想政治工作之一，就是以史为鉴，把学习中国共产党党史和学习贯彻习总书记系列重要讲话精神结合起来，并把这些精神贯彻到促进发展WAPI等自主可控创新技术产业中去。

2021年是中国共产党成立100周年，对于中华民族伟大复兴，百年诞辰恰风华正茂。2021年1月至7月，联盟秘书处结合自身工作实际，通过自学、集体



今天我们将回顾第三个历史时期：翻天覆地 中国共产党在改革开放和社会主义现代化建设新时期推进富国大业（1978年12月-2012年11月）



今天我们将回顾第四个历史时期：惊天动地 中国共产党在中国特色社会主义新时代推进并将在本世纪中叶实现强国大业（2012年11月至今）



学习、专题研讨等形式，开展了中国共产党党史的系统学习。通过集体学习，让秘书处全体同志更加牢记党从诞生到强大，历经磨难，终成大业，百年道路，苦难而光辉。党的发展历程经历了无数的苦难，我们的党也战胜了所有的苦难，没有什么是中国共产人不能克服的，没有什么是中国共产人不能战胜的。秘书处同志们说：苦不苦想想长征两万五。这正是我们党克服艰难险阻的真实写照，是属于我们中国人民

的民族精神，更是中国共产党人的品质。我们学习党史，就要在深刻理解苦难和挫折中坚定理想信念，锻炼意志品质，在任何困难面前绝不低头、绝不认输、不放弃、不抛弃，为自己的共产主义事业奋斗终生！

在此基础上，联盟秘书处同志们还自发开展了4期《学习建党百年，重温峥嵘岁月》的分享和宣传活动，和产业链上下游成员一起，践行“学史明理、学史增信、学史崇德、学史力行”的目标。

联盟秘书处认真学习贯彻习总书记在两院院士大会 中国科协十大上的重要讲话精神

WAPI产业联盟 刘剑昕

2021年5月28日上午，中国科学院第二十次院士大会、中国工程院第十五次院士大会、中国科学技术协会第十次全国代表大会在人民大会堂隆重召开。中共中央总书记、国家主席、中央军委主席习近平出席大会并发表重要讲话。WAPI产业联盟秘书处第一时间组织全体工作人员学习领会总书记的重要讲话精神。

习总书记指出：今年是中国共产党成立一百周年。在革命、建设、改革各个历史时期，我们党都高度重视科技事业。从革命时期高度重视知识分子工作，到新中国成立后吹响“向科学进军”的号角，到改革开放提出“科学技术是第一生产力”的论断；从进入新世纪深入实施知识创新工程、科教兴国战略、人才强国战略，不断完善国家创新体系、建设创新型国家，到党的十八大后提出创新是第一动力、全面实施创新驱动发展战略、建设世界科技强国，科技事业在党和人民事业中始终具有十分重要的战略地位、发挥了十分重要的战略作用。

习总书记指出，当今世界百年未有之大变局加速演进，国际环境错综复杂，不稳定性不确定性明显增加。逆全球化、单边主义、保护主义思潮暗流涌动。这让联盟秘书处同志们更加清晰地认识到：在科技创新成为国际战略博弈的主要战场，围绕科技制高点的竞争空前激烈的今天，我们必须保持强烈的忧患意识，做好充分的思想准备和工作准备。

结合联盟15年在WAPI等网络安全领域的创新经历，秘书处同志们认为习总书记的讲话说到了我们的心坎里：党的十九大以来，党中央全面分析国际科技创新竞争态势，深入研判国内外发展形势，针对我国科技事业面临的突出问题和挑战，坚持把科技创新摆在国家发展全局的核心位置，全面谋划科技创新

工作。坚持党对科技事业的全面领导，观大势、谋全局、抓根本，形成高效的组织动员体系和统筹协调的科技资源配置模式。牢牢把握建设世界科技强国的战略目标，以只争朝夕的使命感、责任感、紧迫感，抢抓全球科技发展先机，在基础前沿领域奋勇争先。充分发挥科技创新的引领带动作用，努力在原始创新上取得新突破，在重要科技领域实现跨越发展，推动关键核心技术自主可控，加强创新链产业链融合。全面部署科技创新体制改革，出台一系列重大改革举措，提升国家创新体系整体效能。着力实施人才强国战略，充分激发广大科技人员积极性、主动性、创造性。扩大科技领域开放合作，主动融入全球科技创新网络，积极参与解决人类面临的重大挑战，努力推动科技创新成果惠及更多国家和人民。

联盟秘书处同志们纷纷表示：作为我国广大科技工作者中的一分子，新形势下，产业联盟的同志们要进一步发挥新型社会组织和创新联合体的优势及独特作用，要以与时俱进的精神、革故鼎新的勇气、坚忍不拔的定力，面向世界科技前沿、面向国家网络安全等重大需求开展各项工作。我们要洞察和把握网络安全大势、发挥WAPI等自主可控技术已有的标准优势、产业优势和市场优势，抢占网络安全自主可控先机，带动全球无线网络和网络安全健康高效发展。我们要直面网络安全技术创新和成果转化过程中的各项问题，发挥联盟公共技术服务平台的作用，迎难而上，推动创新和成果转化，去满足市场需求。我们相信，通过联盟和产业界的协同创新，通过扎扎实实的工作，一定可以肩负起时代赋予的重任，实现我国高水平科技自立自强！

WAPI产业联盟召开2021年第一次理事会和监事会

WAPI产业联盟 周 园

2021年7月7日，WAPI产业联盟召开2021年第一次理事会（总第二十四次）。中国电信集团有限公司、中国联合网络通信集团有限公司、国家无线电监测中心检测中心、国家密码管理局商用密码检测中心、北大方正集团有限公司、西电捷通公司、北京六合万通微电子技术股份有限公司、深圳市明华澳汉科技股份有限公司、北京中电华大电子设计有限责任公司、广州杰赛科技股份有限公司等单位的理事代表出席会议。

理事会议由曹军理事长主持，联盟监事会全程见证。

会上，理事代表听取了张璐璐秘书长汇报的《WAPI产业联盟2020年度工作报告》、《WAPI产业联盟2020年度财务决算报告》、《WAPI产业联盟2021年度工作计划》、《WAPI产业联盟2021年度财

务预算报告》等草案，以及2021年WAPI产业联盟会员大会筹备情况、中关村无线网络安全产业联盟会员大会换届筹备工作情况等。理事代表对联盟工作表示充分肯定，审议通过了上述议题，并委托联盟秘书处提请会员大会审议、表决。会上，理事代表还和联盟秘书处一起，对产业和联盟有关工作进行了讨论。

监事会结合日常对联盟秘书处工作的监督情况给予高度评价。一致认为：联盟严格遵守国家和相关法律法规、严格依照《社会团体登记管理条例》和社会组织管理机构要求、严格遵循联盟《章程》开展各项工作，且成效显著。

当天，还召开了2021年WAPI产业联盟第一次监事会（总第六次）。监事长和全体监事集中讨论并通过了《WAPI产业联盟监事会2020年度工作报告和2021年度工作计划》，将提请2021年会员大会审议表决。

WAPI产业联盟召开2021年会员大会（总第十五次）

WAPI产业联盟 刘剑昕

2021年7月8日，根据WAPI产业联盟《章程》及相关工作安排，2021年WAPI产业联盟会员大会（总第十五次）在北京召开。中国移动通信集团公司、中国电信集团有限公司、中国联合网络通信集团有限公司、国家密码管理局商用密码检测中心、国家无线电监测中心检测中心、北大方正集团有限公司、西电捷通公司、北京中电华大电子设计有限责任公司、北京六合万通微电子技术股份有限公司、广州杰赛科技股份有限公司、深圳市明华澳汉科技股份有限公司、中国电力科学研究院有限公司、华为技术有限公司、高通无线通信技术(中国)有限公司、新华三技术有限公司、北京数字认证股份有限公司、南方电网深圳数字电网研究院有限公司、神州数码云科信息技术有限公司、北京比邻科技有限公司、北京华信傲天网络技术有限公司、鼎桥通信技术有限公司、广西电力线路器材厂有限责任公司、广西通量能源技术有限公司、广西新海通信科技有限公司、广州广电计量检测股份有限公司、南京博洛米通信技术有限公司、瑞晟微电子（苏州）有限公司、深圳航天科创实业有限公司、深圳市瑞科慧联科技有限公司、深圳市智开科技有限公司、深圳市信锐网科技术有限公司、中科开创(广州)智能科技发展有限公司等79家会员单位百余位代表出席会议。工业和信息化部宽带无线IP标准工作组、ISO/IEC JTC1/SC6国内技术对口单位、无线网络安全技术国家工程实验室、北京联盛德微电子有限责任公司、南方电网科学研究院有限责任公司、广州

市智讯达信息科技有限公司、江苏省电子信息产品质量院、深圳市天海万讯科技有限公司、巷子科技（北京）有限公司、北京紫光展锐科技有限公司等单位代表列席会议。

会议由联盟秘书处肖非主持，联盟监事长夏翔全程见证。

受联盟理事会委托，张璐璐秘书长汇报了《WAPI产业联盟2020年度工作报告》、《WAPI产业联盟2020年度财务决算报告》、《WAPI产业联盟2021年度工作计划》、《WAPI产业联盟2021年度财务预算报告》，并提请会员大会审议和表决。2020年，WAPI等自主可控网络安全技术产品在新型基础设施、各重要行业/领域需求旺盛。WAPI产业联盟紧密结合市场需求，依托公共技术平台，组织会员开展创新和成果转化工作，成效显著。截至2020年底，联盟会员单位增至101家；支持WAPI的无线局域网芯片超过500款型号、全球累计出货量超过160亿颗，移动终端和网络侧设备等超过17000款；联盟组织制定（参与制定）并发布（获发布）的标准达134项，其中：国际标准（ISO/IEC）14项、欧洲标准3项，国家标准39项，国家军用标准4项，行业标准7项，团体标准67项。联盟也因产业服务成效突出，荣获“中国社会组织评估5A级”资质，连续第十年以优异成绩通过GB/T19001-2016 idt ISO9001:2015质量管理体系认证，并荣获2020年度中国标准创新贡献奖标准项目三等奖。

张璐璐表示，2020年是WAPI产业“锻长板、

高质量发展”的一年，也是全体会员和联盟一起克服新冠疫情困难，协同创新的一年。这一年，WAPI产业联盟发挥创新联合体作用，组织厂商，服务市场需求；通过标准化、公共技术研发、测试校验等公共服务平台，解决市场和厂商新基建过程中“想做、做不了、但又必须要做的难题”。在市场、产业和联盟的共同努力下，WAPI在“自主可控、技术产业完备、标准化程度高、规模应用标杆全”等方面更具显著优势。2021年是“十四五”开局之年，联盟将聚焦“服务国家安全、自主可控和创新战略”，聚焦“满足市场日益旺盛的安全网络建设需求”，组织联合创新，并从战略沟通、公共技术支撑服务等层面，达成市场和会员的高效对接。

夏翔监事长汇报了《WAPI产业联盟监事会2020年度工作报告和2021年度工作计划》，并提请会员大会审议和表决。监事会认为，秘书处在理事会的领导下，立足于联盟工作现实，着眼于行业长远的未来发展，扎实管理，严格要求，积极进取，锐意创新，为服务联盟会员发挥了重要作用。

与会会员对上述待审事项进行投票表决，均以全票通过。

2021年1至7月，南方电网数字电网研究院有限公司、深圳航天科创实业有限公司、南方电网深圳数字电网研究院有限公司、广西电力线路器材厂有限责任公司、广西通量能源技术有限公司等单位加入联盟，联盟会员单位增至106家。会上，深圳航天科创实业有限公司产品经理蔡隽代表新会员单位发言，介绍了公司业务及对未来的展望。

会上，无线网络安全标准化委员会副主任委员黄振海分享了《新近产业政策分析和WLAN相关

合规体系总结》，对近期公布的和无线网络产业相关的法律、行政法规、技术标准等进行了关联性分析。黄振海强调，当前行业建设关键信息基础设施的基本原则和共识是：应符合网络安全/密码相关法律（密码法、网络安全法、标准化法、数据安全法）、行政法规（商用密码管理条例、网络安全等级保护条例、关键信息基础设施安全保护条例）、规章（行业相关的密码使用要求）要求，应使用符合国家法规和标准规定的技术和产品。

WAPI产业联盟市场总监简练做《服务应用市场的两大抓手——标准与测试》主题报告，介绍了市场用户和企业普遍关心的联盟标准化和测试两大平台，以及服务厂商、用户、检测机构的具体情况。简练表示，WAPI产业联盟开放专业规范，鼓励并欢迎所有有意愿的单位加入，为无线网络和网络安全技术创新贡献力量，并获得应有收益。

会上，联盟还发布了最新版的《WAPI标准产业应用及环境监测报告》。



扫描二维码可直接获取最新版《WAPI标准产业应用及环境监测报告》

WAPI产业联盟召开2021年第二次标准工作及项目组会议 (总第118次)

WAPI产业联盟 肖 非

2021年6月24日，WAPI产业联盟召开2021年第二次标准工作及项目组会议。会议包括：报告2021年第二季度技术标准产业工作、讨论并审议在研标准项目、讨论拟立项项目建议、讨论标准国际化工作、标准化知识交流与培训等。来自中国电信集团有限公司、新华三技术有限公司、华为技术有限公司、西电捷通公司、北京数字认证股份有限公司、北京华信傲天网络技术有限公司、迈普通信技术股份有限公司、南京博洛米通信技术有限公司、中科开创（广州）智能科技发展有限公司、高通无线通信技术（中国）有限公司、瑞晟微电子(苏州)有限公司、北京紫光展锐科技有限公司、广州广电计量检测股份有限公司、巷子科技(北京)有限公司、陕西省网络与信息安全测评中心、重庆电子技术研究所、重庆源盾科技有限公司、四川岁月文明科技有限公司、重庆邮电大学、无线网络安全技术国家工程实验室、ISO/IEC JTC 1/SC 6国内技术对口单位、工业和信息化部宽带无线IP标准工作组等单位的代表参加会议。

WAPI产业联盟秘书长张璐璐表示，第二季度，已立项和在推标准均按计划进行，推进顺利。值得关注的是，团体标准和当下WAPI各行业的市场建设、技术演进、产业升级密切相关，因此无论是厂商和用户方的参与度、征求意见期间的反馈和专题讨论、还是团标与行业标准的联合创新互促等方面，都能感受到市场赋能下联盟创新联合体的活力。目前除南网之外，国网、交通、家电、公安、

国防等行业WAPI建设相继启动，相信标准这个抓手将发挥更大作用。联盟在标准工作中，坚持技术规范与测试规范并重，做好标准联合创新和为市场用户厂商做好公共测试服务；在标准成果转化方面，坚持技术标准与工程化验证工作同步开展，在标准制定过程中就把产业化的路径走通。这也使得，联盟大多数团体标准发布之日，即是相关产品推向市场之时。

无线网络安全标准化委员会副主任委员黄振海表示，随着国家十四五规划和2035年远景目标纲要的逐步落实，在我们标准产业共同体关注的网络通信和网络安全领域，在国际技术演进、国家引导政策、技术标准、产品支撑技术平台、产业/行业方面展现出了新的演进趋势和进展。十四五规划明确提出要健全网络安全法律法规和制度标准，建立健全关键信息基础设施保护体系。加强网络安全风险评估和审查。加强网络安全关键技术研发。强化能源网络安全防护。积极参与数据安全等国际规则和数字技术标准制定，推动构建全球网络空间命运共同体。这些内容，既是我们WAPI标准产业共同体作为国内有代表性的专注于无线网络和网络安全的产业群体的使命，也给我们带来了时代机遇。

WAPI产业联盟市场总监简练报告2021年第二季度联盟标准产业应用工作：WAPI产业联盟成为北京市地方标准《高质量团体标准评价指标体系》联合起草单位；2项团体标准完成报批，即将发布；17项团体标准正在不同阶段推进中，进展顺利；多家厂

商数十款产品通过了联盟测试并获得测试报告；外部媒体宣传与联盟自媒体双管齐下，标准推广宣贯成效显著。

黄振海介绍了第二季度标准化工作情况：在团体标准项目方面，完成报批2项；完成送审2项；形成送审稿10项；形成草案稿5项。在标准国际化方面，SC6国内技术对口工作稳步推进，第二季度共对内流通国际提案文件49份，向国际上反馈投票/意见19份；我国主导的多项国际标准项目取得进展。此外，黄振海受国标委标准审评中心邀请担任拟立项国家标准评审专家并进行了项目评审工作。

无线网络安全标准化委员会委员郑骊做《2021年第一次项目组集中会议要点回顾》报告。她回顾了2021年第一次项目组集中会议决议，通报了上次会议决议的执行情况。

在已立项项目讨论阶段，项目组对已立项的《关键信息基础设施无线局域网技术要求》（第3~4部分，公安、铁路行业）（草案稿）、《无线局域网系统》（第1~3部分，设计、施工、验收）（草案稿）、《关键信息基础设施无线局域网测试方法第1部分：通用要求》（送审稿）、《信息技术 系统间远程通信和信息交换 原子密钥建立与实体鉴别》（第1~7部分）（送审稿）、《GB/T 32420实施指南 第2部分：无线局域网设备测试》（送审稿）、《无线局域网接入控制》（第1~2部分）（送审稿）、《信息安全技术证书管理测试规范》（送审稿）、

《WAPI证书管理方案研究报告》等进行了介绍，与会专家针对上述标准进行了热烈讨论，并根据会上意见形成了相关决议。

在拟立项项目阶段，西电捷通公司张变玲代表《无线局域网产品工程化实现指南》系列团体标准项目组介绍修改单项目的提案原因和主要内容，介绍已形成的修改单征求意见稿，会议批准该项目尽快开展。岁月文明科技公司朱桢代表项目组介绍《未来网络架构 第1部分：基于服务质量的代理模型》、《未来网络 协议与机制 第2部分：基于服务质量的代理模型》草案稿和立项建议，会议批准该项目启动立项审批流程。

在标准国际化工作方面，ISO/IEC JTC 1/SC 6国内技术对口单位秘书处李玉娇报告了二季度SC6标准国际化工作进展情况，并在标准化知识交流与培训环节介绍了国际标准会议注册流程，为与会专家未来参与标准国际化工作提供有效信息。

WAPI产业联盟3项无线局域网系统/工程团体标准正式立项

WAPI产业联盟 刘剑昕

2021年6月，经WAPI产业联盟无线网络安全标准化委员会评审，《无线局域网系统 第1部分：工程设计规范》、《无线局域网系统 第2部分：工程施工规范》、《无线局域网系统 第3部分：验收测试方法》等3项无线局域网系统/工程系列团体标准正式立项。多家单位积极申请成为参编单位。

多年来，为持续推动安全无线局域网的规模应用和发展，WAPI产业联盟联合产学研用各单位和国内外标准化组织，以GB 15629.11系列国家标准为基础，从总体、基础技术、组网技术、网络管理技术、产品及测评、应用六个方面规划布局，构建了比较完整的基于WAPI的无线局域网国家/行业/团体标准体系，已发布各类标准55项。

当前，随着WAPI在各行业的规模应用，网络建设方和用户方都迫切需要一套可依据的安全无线局域网系统设计、工程实施的标准，但目前国内外这类标准比较缺乏。为此，联盟牵头组织了本系列团体标准的创新工作。

本系列团体标准依据网络安全法、密码法和等保2.0等相关法律法规以及GB 15629.11系列国家标准、GB/T 32420—2015《无线局域网测试规范》等标准，针对WAPI安全无线局域网在行业领域实际建设中的工程施工规范要求，规定了相应的施工过程要求、施工规范要求等，为行业内WAPI网络的设计规划建设单位提供了技术支撑，保障了WAPI无线局域网系统工程施工的科学规范，促进了WAPI高质量发展。

WAPI 产业联盟 (中关村无线网络安全产业联盟)

NO4451【WAPIA-2021086-通知】

关于《无线局域网系统 第1部分：工程设计规范》 等3项团体标准立项的通知

各会员及有关单位：

根据 WAPI 产业联盟《团体标准制修订工作程序》的有关规定，无线网络安全标准化委员会对《无线局域网系统 第1部分：工程设计规范》、《无线局域网系统 第2部分：工程施工规范》、《无线局域网系统 第3部分：验收测试方法》团体标准进行立项评审，根据评审意见，上述3项标准符合立项条件，现批准立项。

希望各单位积极参与标准项目的制定，并严格按照联盟标准化工作要求，做好标准项目的组建、标准的起草等工作，确保标准制定质量和水平及适用性和实效性，按期完成标准编制相关工作。



本系列团体标准立项之后，各参编单位积极贡献并迅速形成了草案稿。2021年7月16日，WAPI产业联盟组织召开了无线局域网系统/工程系列团体标准项目组工作会议，来自国家信息技术安全研究中心、无线网络安全技术国家工程实验室、西电捷通公司、广州广电计量检测股份有限公司、工业和信息化部宽带无线IP标准工作组等单位的专家参加会议。与会专家就项目草案稿的完成情况、分工意向及下一步工作计划进行了充分讨论。会后，有更多设备、终端厂商和测试机构向联盟标准化部表达了参与意向。

WAPI产业联盟2项无线局域网接入控制团体标准进入送审阶段

WAPI产业联盟 肖 非

无线局域网接入控制 第1部分：组网架构规范

Wireless LAN Cloud Access Control part 1: Networking Architecture
Specification[©]

无线局域网接入控制 第2部分：调度平台技术规范[←]

Wireless LAN Cloud Access Control part 2: Technical Specification for
Dispatching Platform[©]

日前，WAPI产业联盟2项团体标准《无线局域网接入控制 第1部分：组网架构规范》和《无线局域网接入控制 第2部分：调度平台技术规范》，经两轮公开征求意见和意见处理，进入送审阶段。提案的主要贡献单位包括中国电信、WAPI产业联盟、西电捷通公司和新华三。

无线局域网（WLAN）组网存在大规模设备管理、部署和维护等重要需求。传统的WLAN大规模部署通常采用按区域部署接入控制器（AC）、接入点（AP）注册到指定AC的模式。当规模部署WLAN网络时，面对数量众多、不同区域的接入点（AP），如何更加合理、更加智能地为其分配最佳的接入控制器（AC），让WLAN网络规模部署和运营更加便捷高效并降低成本，成为规模部署WLAN网络的关键要求之一。WLAN云管理技术是构建运营级WLAN网

络的核心关键技术，通过云AC组网架构，实现了接入点（AP）更加灵活智能地接入合适的接入控制器（AC），有利于构建"大容量、高可靠、可管理、可扩展"的运营级WLAN网络。该技术对现有WLAN规模部署给予了有效补充和完善，极大地提升了设备管理、部署和维护效率，市场潜力巨大。

WAPI产业联盟是国家标准委首批团体标准试点单位，多年来持续组织和推动"标准制定、标准成果转化、标准走出去"等工作。在联盟创新联合体的共同努力下，在标准化方面，已开展了170余项标准的制修订，为构建最基础最共性的网络安全架构体系提供有效支撑，其中发布（获发布）国际标准（ISO/IEC）14项、欧洲标准3项、国家标准41项、国家军用标准4项、行业标准7项、团体标准68项。

WAPI产业联盟成为北京市地方标准 《高质量团体标准评价指标体系》联合起草单位

WAPI产业联盟 肖 非



2021年5月26日，北京市质监局标准化处和北京市标准化研究院组织WAPI产业联盟等在团体标准制修订方面具代表性的10余家社团单位，召开了北京市地方标准《高质量团体标准评价指标体系》（以下简称《评价体系》）项目启动会。

会议由北京市标准化研究院田川主任主持。田川重点介绍了《评价体系》的技术内容与指标。北京市市场监管局标准处李永华处长和李凌松副处长共同就《评价体系》的研制目的、意义和适用范围进行了具体解读，提出希望依托《评价体系》推动高质量团体标准的可持续性发展及在行业中的普及和应用；探索促进社会第三方检验检测、认证机构积极采用高质量团体标准开展检验检测、认证工作，提高检测、认证的可靠性和水平；探索建立团体标准采信机制，在政府采购中鼓励使用市场自主制定的团体标准等。

WAPI产业联盟结合《评价体系》（草案）提出

自身建议，并和与会单位进行了研讨和交流。会上，确定WAPI产业联盟、中关村半导体照明工程研发及产业联盟、北京市闪联信息产业协会、北京电信技术发展产业协会等单位作为《评价体系》的联合起草单位，计划于2021年内发布。

产业联盟这类创新联合体，在响应和服务市场需求、组织技术标准协同创新、推动成果转化等方面具有先天优势。目前北京有很多优秀的产业联盟，在标准创新尤其是团体标准的探索和先试先行方面成果突出。2019年，国家标准化管理委员会、民政部联合印发了《团体标准管理规定》（国标委联〔2019〕1号），从规范、引导和监督团体标准化工作出发，对团体标准的制定、实施和监督提出了更加具体的要求，北京、上海、浙江、广州、深圳等地迅速响应，对相关工作予以细化和落实。

WAPI产业联盟组织会员参加 2021“科创中国”科技创新企业家高峰论坛

WAPI产业联盟 刘剑昕

7月27日，WAPI产业联盟组织会员单位参加第二十三届中国科协年会“科创中国”科技创新企业家高峰论坛。

论坛以“新兴产业与高质量发展”为主题，由中国科学技术协会和北京市人民政府共同主办，中国科协企业创新服务中心和中关村产业技术联盟联合会承办，搭建跨界交流平台，聚焦前沿科技和新兴产业领域，共商高成长性企业开放信任合作之举，共谋高水平科技自立自强之策，助力北京国际科技创新中心建设。

在论坛筹备期间，WAPI产业联盟积极响应中关村产业技术联盟联合会号召，向会员单位介绍了会议概况、日程和关注重点等。在论坛组织方面，联盟秘书处委派专职人员积极协助会务组开展相关工作，确保论坛在安全防疫的基础上高质量召开。论坛召开当天，联盟秘书处负责同志和十余家会员代表出席论坛，还有多家外地会员专程来京参会。

中国科协党组成员、书记处书记吕昭平出席并致辞，美国旧金山湾区委员会主席兼首席执行官吉姆·旺德曼视频致辞。中国工程院院士樊代明、中国工程院院士沈昌祥、国际科技园及创新区域协会副主席陈鸿波、中泽嘉盟投资有限公司董事长吴鹰等嘉宾出席。来自科技界、产业界、投资界160余位专家学者和全国学会、联盟代表现场参加。

吕昭平在致辞中指出，当前数字经济成为促进全球经济高质量发展的新动能，绿色产业发展成为推动全球经济复苏的新力量，融合发展新趋势催生企业创新范式深刻变革。本次论坛深入贯彻落实习总书记重要讲话精神，坚持包容可持续发展，把握科技创新机遇，围绕产业链部署创新链，围绕创新链布局产业链，构建以企业为主体的技术创新体系，不断提升企业科技创新能力，以开放信任合作推进科技进步实现价值共赢，以产学研深度融合构建科技创新体系新范式，顺应经济全球化潮流，加强合作，应对风险挑战。他强调，中国科协愿携手科技界、产业界、投资界，共同推进“科创中国”建设，努力搭建产学研政金对话沟通、融通合作的桥梁，共同服务企业创新发展，共同助力北京国际科技创新中心建设，共同推进京津冀协同发展，为加快构建新发展格局、推动经济高质量发展贡献力量。

樊代明、沈昌祥、陈鸿波、吴鹰分别以“疫后医学发展的思考”“数字经济时代的机遇与挑战”“科技创新生态系统的构成与案例”“5G与人工智能”为





题作主旨报告。

中国科协企业创新服务中心主任苏小军在论坛总结中指出，当前正处于未来已来、唯变不变的时代，本次论坛邀请科技界、产业界、投资界精英开展高水平跨界交流，共同探讨新兴产业发展趋势和高质量发展对策，将对推动全球科技创新合作起到良好促进作用。

2006年3月成立的WAPI产业联盟（中关村无线网络网络安全产业联盟），是注册并扎根于北京市中关村15年的创新联合体，是国内最早一批从事网络安全技术产业创新且成果显著的社会组织，更是当前服务北京科创中心建设、深化科技体制改革、促进各类主体协同创新的排头兵。多年来，联盟密切关注北京市和中关村国家自主创新示范区的战略发展及重点关注，发挥了科技类社会组织在各类主体协同创新中的协调服务作用：通过整合协调产业和社会资源，提升了联盟会员在无线网络和网络安全相关领域的研究、开发、制造、服务水平，促进了产业健康发展；以国际领先的基础共性技术TePA和WAPI，带动了无线网络和网络安全产业健康高效发展，促进了产业群体协同创新、提升了综合竞争力。



南网深圳数研院WAPI系列产品通过联盟测试

WAPI产业联盟 王立华



2021年6月，南方电网深圳数字电网研究院有限公司（以下简称深圳数研院）的无线局域网系列产品通过了WAPI产业联盟无线局域网鉴别与保密基础结构（WAPI）互通性、完整性及性能测试。联盟为上述产品出具了测试报告。

本次测试通过的设备包括室内/室外无线接入点（AP）、接入点控制器（AC）、鉴别服务器（AS）、客户前置设备（CPE）以及WPAI摄像头设备。其中，AP、CPE设备均支持2.4/5GHz双频接入，通信速率支持802.11ac协议，AS设备具备漫游功能，可满足行业应用中宽带、移动性、大连接的无线局域网应用需求。

期间，联盟实验室依据无线局域网产品鉴别与保密基础结构（WAPI）功能测试项目（2020年11月版），进行了协议互通性、完整性、功能及性能测试。测试过程中，联盟实验室和设备厂商通过远程联调形成紧密互动。联盟实验室结合用户单位的行业特点和管理要求，对设备管理界面和相关功能提出了整改意见，深圳数研院快速对问题进行了整改，完善并提升了产品功能。

据深圳数研院介绍，本次测试通过的WAPI系列产品，将用于输电线路安全监测、故障定位、安全巡检等业务。

西电捷通公司国产平台WAPI鉴别服务器通过联盟测试

WAPI产业联盟 王立华

2021年7月，西电捷通公司的国产平台WAPI鉴别服务器通过了WAPI产业联盟无线局域网鉴别与保密基础结构（WAPI）互通性、完整性测试。联盟为上述产品出具了测试报告。

据西电捷通公司介绍，该WAPI鉴别服务器的软硬件平台采用了国产安全操作系统和国产高性能多核处理器（CPU），能有效满足党政军以及金融、税务、交通、能源、电信等重要行业的自主可控需求。该产品集成了证书签发服务单元（CISU）和鉴别服务单元（ASU），其中CISU支持终端实体证书管理（CMEE）功能，通过该功能用户可自主生成密钥并在线获取证书，实现证书自动下载功能。更值得一提

的是，该产品具备以太网安全TLSec（TLSec是我国自主创新的以太网安全技术）的身份鉴别能力，支持TLSec证书管理及鉴别服务，可在线对光/电以太网终端和以太网安全控制器的安全连接进行身份鉴别，从而为用户提供有线无线一体化安全鉴别服务。

联盟实验室依据无线局域网产品鉴别与保密基础结构（WAPI）功能测试项目（2020年11月版），对上述产品进行了WAPI协议互通性、完整性测试。测试过程中，联盟实验室与产品厂商通过远程联调的方式，顺利完成了各测试项目的配置和测试。后续，该产品将在信息技术应用创新等领域发挥自主可控和保障本质安全的作用。

西电捷通公司WAPI无线接入鉴别综合网关通过联盟测试

WAPI产业联盟 王立华

2021年7月，西电捷通公司的WAPI无线接入鉴别综合网关(以下简称WAPI网关)通过了WAPI产业联盟无线局域网鉴别与保密基础结构（WAPI）互通性、完整性及扩展功能测试。联盟为上述产品出具了测试报告。

该WAPI网关同时支持AP、AS和CIS功能，能够为用户提供证书管理、身份鉴别和无线接入一体化服务，可满足独立构建/临时快速组建小规模（100用户以内）完整WAPI无线局域网络的需求。此外，该WAPI网关还支持终端实体证书管理（CMEE）扩展功能，通过该功能可配合终端自主生成密钥并在线获取证书，实现证书自动下载功能。

据西电捷通公司介绍，该产品叠加了IP安全可信

TISec终端功能，能提供远程IP安全接入能力，可实现跨互联网建立IP端到端安全连接。更值得一提的是，该设备内嵌WAPI硬件密码安全协议模块，该硬件模块已通过国家权威机构检测认证，能够防止物理攻击，结合可信主动度量技术，可满足高安全、高性能的行业市场需求。

目前，联盟实验室已依据最新版无线局域网鉴别与保密基础结构（WAPI）功能测试项目（2021年07月版），对上述产品进行了WAPI协议互通性、完整性及扩展功能测试。针对此类同时具备多种功能的设备，联盟实验室会对不同种类的功能（AP、AS和CIS）进行分别测试，并分别出具AP、AS和CIS的测试报告，作为此类设备在行业应用中的采信依据。

华信傲天发布高性能无线局域网接入点产品

WAPI产业联盟 简 练

日前，华信傲天发布高性能无线局域网接入点产品-AP351。

该产品符合GB 15629.11系列无线局域网国家标准和T/WAPIA 007.10—2020《无线局域网产品工程化实现指南 第10部分：WAPI与IEEE 802.11ax》团体标准，支持2.4GHz & 5GHz双频工作，拥有16个无线空间流，其中2.4GHz支持4×4:4，5GHz支持8×8:8+4×4:4 UL/DL MU-MIMO以及搭配了全新物联网BLE5.0模组，整机创新性支持10.75Gbps的峰值速率，支持同时超大规模1536个关联终端。产品设备支持10GE+10GE高速冗余上行接口，满足苛刻场景下的高质量应用体验，可广泛应用于大型会议中心、文体场馆、公共交通场馆等终端密度高和高带宽视频业务密集的场景。

据介绍，作为WAPI联盟成员以及无线网络安全标准化委员会成员，华信傲天非常重视网络安全和自主创新，在SM4等国产安全加密算法方面也保持密切关注，目前其全系列产品均符合WAPI标准。

迈普通信以双第一中标中国电信集采

迈普通信

2021年5月20日，中国电信集团有限公司发布《中低端路由交换设备（2021年）集中采购项目中标候选人公示》，迈普通信凭借优秀的产品和服务，以双第一的成绩中标中低端路由器、中低端交换机两个标包。

迈普通信连续多年入围运营商集采，产品广泛应用于电信、移动、联通等运营商自建网和各类ICT场景中，且保持有较高的市场份额。近两年，迈普先后在中国移动《2020年至2021年低端路由器和低端交换机集中采购》、《2021年至2022年数据中心管理交换机集中采购》中获得优异成绩。

此外，迈普还是中国信创网络设备领先品牌，在党政、金融等行业具一定应用规模。

新华三中标中国移动高端路由器和高端交换机集采项目

新华三

2021年6月，中国移动公布了2021年至2022年高端路由器和高端交换机产品集中采购中标结果，紫光股份旗下新华三集团中标三个标段，其中标包3的项目以29%份额中标，在标包7和标包8的项目中同时以70%的第一份额中标。

伴随着超高清视频，云计算等业务的发展，数据流量激增，网络宽带的承载能力面临严峻的考验，这一现状催生了市场对高端路由器和高端交换机的迫切需求。目前新华三集团已拥有适配运营商IP网络各场景的高端路由器产品，产品秉承“电信级”可靠性的传统，拥有自主知识产权的通用Comware操作平台，采用分布式的组件化灵活架构，有效地将诸多技术完美融合，结合创新的全分布式NP/多核架构体系，使得新华三路由器实现了业务灵活性和高性能硬件转发的有机结合。本次标包3项目的中标产品——CR16018-F是由新华三自主研发的高端路由器，路由转发性能能够满足用户现在以及未来业务扩展的需求。目前，CR16000产品已经连续多年入围并落地中国移动云专网集采全部标段。

数字认证蝉联“中国网络安全百强”领军者行列

数字认证

6月16日，在网安之光·网络安全发展论坛现场，数世咨询发布了《中国网络安全百强报告(2021)》（以下简称百强报告）。北京数字认证股份有限公司继2020年后再度入选，居领军者行列。

据介绍，百强报告通过品牌影响力、企业规模、技术创新力三大维度，从700多家经营网络安全业务的企业中遴选出综合实力较为突出的100家企业，誉为“综合实力百强”。百强企业共分为领军者、竞争者和挑战者三类。

据数字认证介绍，20年来以建设网络强国为己任，以创新发展为理念，勇于承担商用密码产业发展重任，共牵头和参与了国家重点研发计划“网络空间安全专项”、国家自然科学基金、发改委国家信息化试点工程、发改委信息安全专项、科技部科技支撑计划、863计划、工信部工业互联网创新发展工程等60余项国家及省部级重点课题。牵头和参与了150余项网络安全国家标准和密码行业标准的制定。曾获得国家科学技术进步奖二等奖、党政密码科技进步奖二等奖、北京市科学技术奖三等奖、重庆市科学技术奖三等奖等多项国家级、省部级荣誉。

华为最大的网络安全透明中心启用

华为

华为最大的网络安全透明中心5月在东莞正式启用。

近两年，行业数字化、人工智能等新技术的发展，及疫情带来的数字化新常态，共同加速了数字世界的到来。网络空间日益复杂，人们在享用数字世界带来的便利的同时，正面临着网络空间中的前所未有的风险和威胁。华为轮值董事长胡厚崑表示，“在这种新常态下，华为呼吁各方在治理架构、标准与技术、验证等专业领域积极合作，共享成功实践，提升整体能力，以增强政府监管部门乃至全社会对网络安全的信任 and 信心，共谋数字化时代发展与安全的解决之道。”

在启用仪式上，华为发布了《华为产品安全基线》白皮书。该基线是华为基于过去十年管理产品安全的实践经验，并参照广泛的外部法规、技术标准、监管需求而提炼形成的。

美国国土安全部将发布首份管路系统网络安全指令文件

互联网安全内参 华盛顿邮报

美国国土安全部正着手发布首份输送管道行业网络安全监管法规，旨在防止5月科洛尼尔公司（Colonial）遭遇重大攻击事件所引发的东海岸燃料供应短缺问题。这次事件凸显了关键基础设施在面对网络攻击时不堪一击的现状。国土安全部高级官员称，该部下辖运输安全管理局将于5月发布安全指令，要求各管路企业向联邦政府当局上报网络事件。官员们还强调将在未来几周之内，针对各管路公司系统的网络防御体系及黑客攻击应对措施，制定出一份更为完善的强制性要求。此前，相关文件均为自愿遵守。

5月中旬，勒索软件攻击导致科洛尼尔油管公司输送管路瘫痪达11天，直接导致美国东南部（包括华盛顿特区）出现供油短气与恐慌性囤积。如果持续时间进一步延长，高度依赖柴油供应的航空公司、公共交通与化学精炼设施都将受到影响。科洛尼尔公司首席执行官表示，该公司被迫向勒索团伙支付440万美元才得以赎回系统控制权。官员们透露，此次网络攻击直接促使国土安全部长Alejandro Mayorkas及其他多位高层官员认真思考如何运用现有运输管理局职能推动行业变革。国土安全部发言人Sarah Peck在一份声明中提到，“拜登政府正采取进一步措施，希望更好地保护美国国内的关键基础设施。运输管理局与网络安全及基础设施安全局正开展密切合作，包括与管路行业各企业进行协调，以确保他们采取一切必要手段增强自身网络威胁抵御能力、保护系统安全运转。”

姗姗来迟的管路系统网络安全指令

运输管理局全面接手管路安全工作始于911事件之后。2001年11月11日，联邦政府着手对运输管理局进行改革，将以往由交通运输部负责的燃料、天然气及化学药品输送管路（当时管路被视为一种运输载体）安保责任移交给新建立的运输管理局。到2010年，美国第一份与网络相关的保护指南才正式出台。这份指南后续虽在2018年经历了更新，但仍未能满足许多专家的预期。大部分关键基础设施部门（包括大坝、医疗保健乃至水处理系统）都还没有任何强制性网络标准，只有大型发电厂与核电站在这方面做出过少量探索。由于美国商会的强烈反对，国会在2012年提出的强制性要求最终未能通过。

新指令将强制执行，按效能评判

运输管理局此次发布的新安全指令要求各管路公司向运输管理局与网络安全及基础设施管理局及时上报网络安全事件，指派一位网络官员（例如首席信息安全官），并准备一部24/7全天候安全联络电话。指令还要求企业根据现有网络准则评估系统的实际安全性，将以往的自愿性标准转为强制性守则。一位资深人士解释道，“这只是第一步，未来还会出台更为强硬的指令，提出更多更具现实意义、能够随技术变化而灵活调整、持久保持有效的新要求。”官员们还提到，新规定有望在未来几周内起草完成，将要求各企业纠正现有问题并解决安全漏洞，否则将面临经济处罚。对于运输管理局，这意味着其执法工作将由管路公司自由配合转为强制执

行。目前的运输管理局指南已经列出部分安全措施要求，例如定期检查远程网络连接。专家们强调，“基于效能”的评判机制可能更为可取。专家们认为，这种方式能够引导企业明确关键目标、持续推动创新并紧跟技术发展趋势。

运输管理局监管能力面临挑战

多年以来，人们对于管路系统遭遇的网络攻击及自身安全缺陷愈发关注。2011年与2012年，针对天然气管路企业的大规模网络入侵活动震惊了整个行业，也促使运输管理局及管路行业努力更新安全标准。但这些标准只要求从业厂商自愿遵守，意味着公司完全可以明确拒绝运输管理局提出的安全制度审计提议。为此，运输管理局于2018年开始推动“验证有效的架构设计审查”，希望借此提高企业的网络响应能力与效率。这项审查计划由网络与基础设施安全局联手爱达荷州国家实验室共同建立。但作为监管机构，运输管理局目前面临的一大挑战，在于严重缺乏能够处理审计与执行工作的资深人才。2014年，运输管理局的管路安全部门雇员只有1名；直到2019年，雇员数量也刚刚达到5人。为此，国土安全部正计划让网络与基础设施安全局同运输管理局合作实施新规则，同时放开更多员工雇用名额——运输管理局可额外招聘16人，网络与基础设施安全局可再招聘100人。Harrell强调，“运输管理局肩负着神圣的使命，多年来为公众安全保障做出了重大贡献。但该局目前确实不具备管理强制性管路安全合规制度的专业知识和必要资源。”因此，他认为国会需要“加快脚步”，并为运输管理局提供丰富的补充性资源。



航天科创：

基于WAPI的变电站多光谱智能巡检系统

深圳航天科创实业有限公司 马天宇

一、变电站现状及背景

随着电网的发展，变电站数量快速增长，而人力资源补充滞后，人员相对紧缺、平均工作量增加，加之缺乏有效的科技手段弥补人力紧缺问题，设备巡视密度必然下降，工作效率降低，电网企业生产力不足的矛盾日益显现，电网企业数字化转型势在必行。变电站少人化、无人化的发展趋势，亟需借助科技手段辅助电网企业对变电站设备的巡视管理。当前，WAPI安全无线局域网技术、5G通信技术、云技术等前沿科技的快速发展，为电网企业数字化转型提供有利条件，全方位研发变电站巡视系统，辅助人工对变电站设备进行巡视，可在短期内解决人员紧缺、变电站设备巡视质量下降等现场实际问题。当前，变电站广泛采用变电站巡检机器人辅助人工开展变电站巡视维护工作，但是机器人巡检对环境适应性、续航能力、障碍规避、高处设备检查等方面表现不足，需要研发新型巡检系统增强现场智能巡检的实用性。

二、变电站多光谱智能巡检系统的研发

航天科创采用军工导弹红外识别技术和自主可控的WAPI无线接入协议安全无线局域网技术，应用于变电站多光谱智能巡检系统的研发，较好地完善了变电站巡视管理体系。通过高处安装的多光谱高清摄像头，对全站范围内设备设施进行扫描，采集站内设备运行状态信息；通过前端摄像头采集的巡检信息，在巡视主机系统进行分析，判断设备运行是否正常，达到智能预警目的；并通过曲线、报表、预警窗格信息条等多种形式展现巡检结果。该系统的研发，弥补了当前变电站巡检工作存在的不足。

三、系统组成

变电站多光谱智能巡检系统主要由多光谱数据采集系统、网络通讯模块和智能分析平台等三部分组成。系统架构由采集感知层、网络传输层、站内平台层组成，系统架构图如下图所示：



图1：系统技术架构图

采集感知层：由各种感知设备和接入网组成，包括各种采集终端和WAPI无线接入网络，采集获取的设备状态、运行环境等信息均可通过WAPI无线网络进行安全可靠传输。感知层设备主要为多光谱云台摄像机（150米超长距离拍摄）、智能传感器、气象信息采集模块，用于实现对目标设备的温度、外观、运行参数及环境数据的采集。如下图所示：

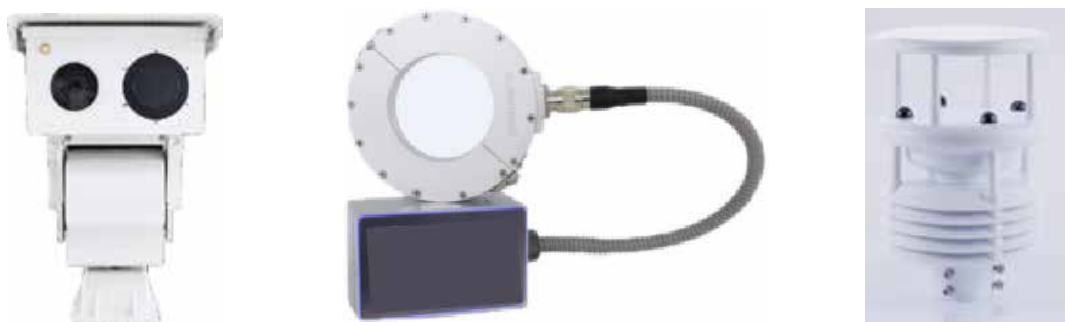


图2：多光谱云台摄像机 智能传感器 气象信息采集模块

网络传输层：网络传输层设备通过TCP、UDP协议传输感知层获取的设备信息，可实现不同类型的感知设备的数据回传至后台主机。

站内平台层：站内平台层主要是对感知层采集的信息进行处理，具备存储、分析及交互展示功能；提供通用计算、存储、智能算法等资源；针对不同的设备，提供故障诊断模型、缺陷图像库、智能决策库等服务；支持应用功能模块建设，大屏、PC端和手机 APP 等各种展示方式的统一访问，提供身份认证、访问、功能配置等管理功能。

四、主要功能

变电站多光谱智能巡检系统具备设备红外检测、火灾预警、现场管控、安防功能、智能分析、联合机器人巡检等多项功能。

1 联合巡检

在变电站内高、中位置安装若干固定式高清摄像机，配合地面智能巡检机器人，形成高、中、低搭配、立体巡检智能物联模式。将检测数据通过数据传输模块传输至智能管控中心，由智能数据处理模块完成数据分析研判，并形成结论，最终在变电站内形成高、中、低错位交互、动静互补、整体定位与局部精准检测相融合、数据无损远距离传输、智能化分析研判的空间立体智能巡检系统，并且可扩展巡检模块。

科创室外巡检机器人：站内部署室外智能巡检机器人1套，主要进行设备表计识别及红外测温工作，按照其自定义规则进行巡视工作，机器人平台软件署巡检点位2564个，目前软件平台调试阶段，部署室外机器人巡检点位1251个。



图3：变电站巡检机器人

2 红外检测

多光谱云台摄像机采用长焦红外光学系统，不受环境温度影响，通过远距离红外扫测对电力设备进行温度测量并分析，通过高低温光标自动追踪功能直观地展示温度极值。远距离测温可根据目标物的距离，自动匹配距离模型参数，校正不同距离目标物的温度偏差；同时，系统可进行任意的点、线、面多区域温度检测。如下图：



图4：多目标温度检测

3 智能识别

变电站多光谱智能巡检系统具备对变电站设备的外观及标识牌、断路器、隔离开关的分合状态，变压器、断路器、互感器等充油、充气设备的油位、压力，避雷器泄漏电流等指示表计的读取。如下图：

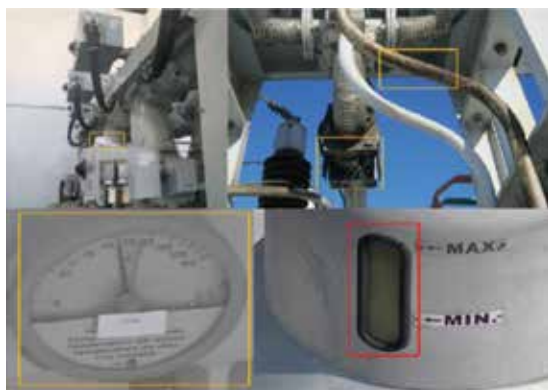


图5：设备智能识别

4 安防监测功能

全时扫描工作模式下，所有多光谱云台摄像机快速转动扫描站内区域，一旦发现外物入侵，系统自动弹窗报警，同时调用最近的云台自动跟踪，直到下一个离入侵物最近多光谱云台摄像机补位跟踪，其他无关多光谱云台摄像机继续保持全时扫描，既保证跟踪轨迹完整，又不影响全时扫描整体工作区位。同时利用多光谱云台摄像机的可见光与红外光摄像头长波红外夜视功能，确保夜间仍然有效监测，实现全天时变电站内安防监测。

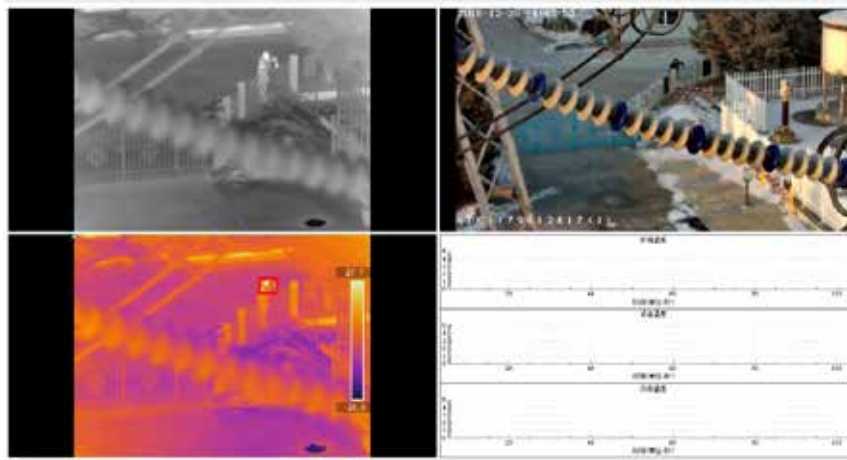


图6: 目标移动侦测

5 智能分析

智能分析功能主要体现在将感知层采集的温度、声音、设备外观、表计读数等信息，与正常数据限值进行对比，分析设备是否正常；与云端缺陷库对比，进一步判断缺陷程度。对于测温数据，系统自动调用DL/T 664—2016《带电设备红外诊断应用规范》，对发热设备缺陷进行智能诊断，判别缺陷性质，同时对运维人员进行提示，从而实现对设备运行状态的智能预测、报警、辅助决策等功能。



图7: 诊断分析、位置提示

6 火灾早期预警

变电站多光谱智能巡检系统在任意工作模式下，所有多光谱云台摄像机具备火灾检测功能，系统根据感知层设备检测的信息，根据火情特征进行预警。

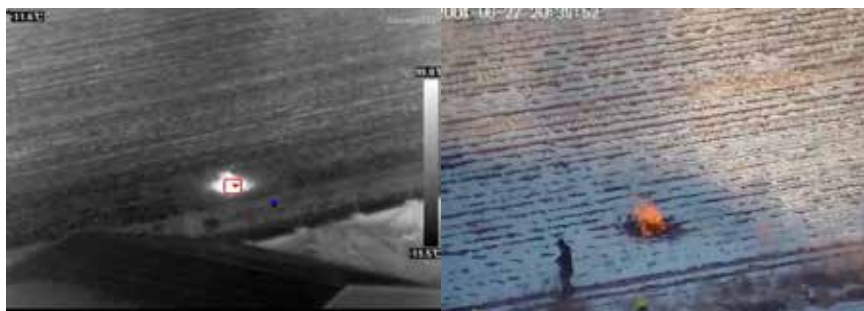


图8: 火情报警

7 现场管控

变电站多光谱智能巡检系统在多光谱云台摄像机定点区域监视工作模式下，将多光谱云台摄像机定位到站内作业区域，设置虚拟围栏后，可对设定区域进行监控，对人员违章越界、未佩戴安全帽、未穿工作服等违章行为及时记录并告警。

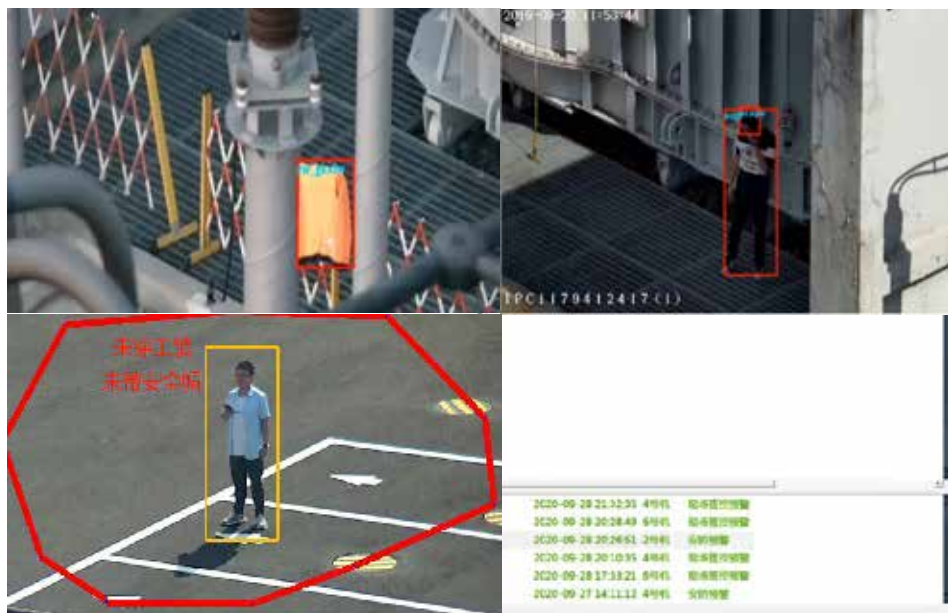


图9: 火情报警现场管控

8 联动机器人巡检

变电站多光谱智能巡检系统在全时扫描、预置位扫描模式下，一旦发现设备异常，即可向巡检机器人发出巡检指令，联动巡检机器人到异常位置做进一步检查。多光谱云台摄像机固定安装在高处，自上向下扫描检测；机器人自下向上，抵近观察，弥补视角缺陷，进一步降低误判率。

五、现场应用

变电站多光谱智能巡检系统推出以来，进行了大量的数据测试，在国内部分变电站进行了布署安装。

1 数据统计

1) 运行数据统计

某变电站初步实现了巡视、红外检测、火灾早期预警、智能分析和现场管控功能。其中，巡视主要包括设备外观、表计、状态、关键设备接头测温工作。在系统运行期间，对系统巡视与人工巡视情况进行数据收集汇总，如下表所示。

系统与人工巡视次数情况（2020年12月1日至2021年4月1日）

巡视模式	巡视周期	单次巡视时间	巡视次数	监测设备总时长
系统预置位巡检	每天4次	2小时	484	968
人工例行巡检	每天1次	1.5小时	121	181.5
人工夜间巡检	7天1次	1小时	17	17
人工全面巡检	15天1次	7小时	8	56

2) 巡检工作量对比

从数据分析可以看出，多光谱智能巡检系统巡视总次数明显多于人工巡视总次数，巡视密度更大；系统监测设备总时长约是人工巡检总时长的4倍，在线时间更长，更全面掌握变电站设备运行状态。

六、具备提前发现设备异常能力

案例1：某变电站多光谱智能巡检系统在发现严重缺陷一处，2021年03月17日16时41分，系统进行红外检测时发现220kV南西甲线1113CT开关侧接线板B相温度异常（80.7℃），并报警，人工复测温度为80.6℃，温度确实存在异常，属于电流致热缺陷，系统具备发现设备过热异常的能力，见图10。

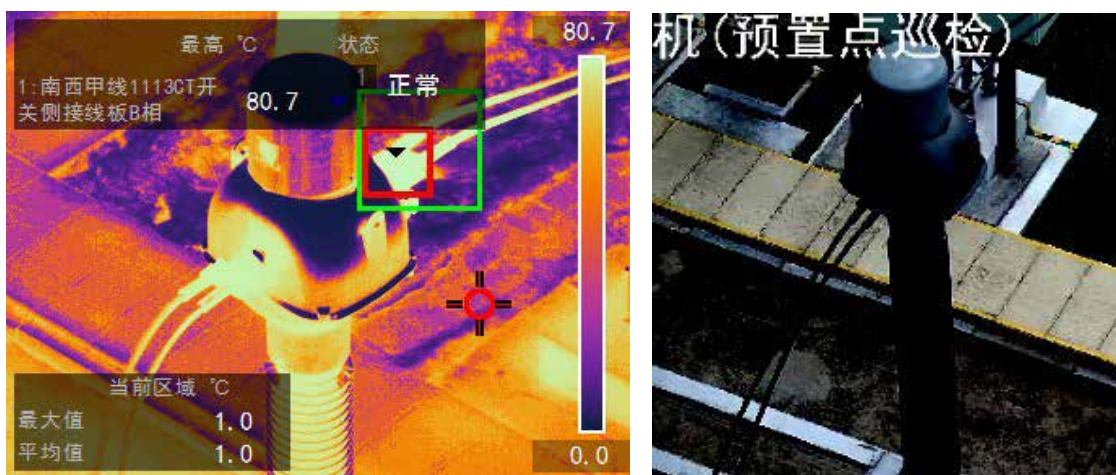


图10: 多光谱智能巡检系统巡视发现缺陷

案例2：2019年4月，某电站685B相电流互感器异常发热，测量发现A相：30.2℃，B相：36.1℃，C相：29.4℃，当时检测环境温度为7℃，判断为设备异常发热，见图11。



图11：多光谱智能巡检系统巡视发现缺陷

案例3：2019年1月，500kV某变电站1号主变备用项，1号主变检修动力箱正上方220kV汇流母线C相T型线夹热点温度73.3℃，正常温度应该为-12℃，当时检测环境温度为-18℃。现场临停处理发现，抱箍处存在断股、破股严重，见图12。

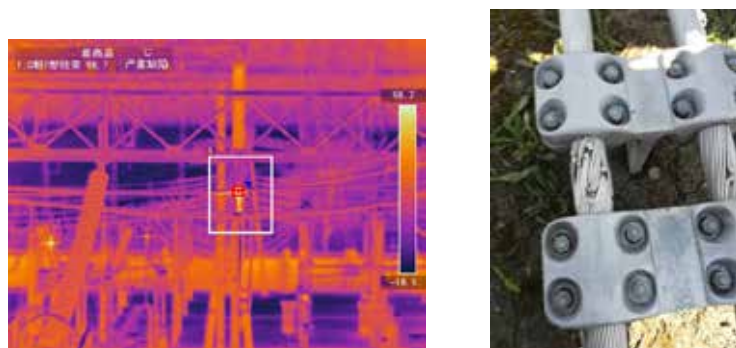


图12：多光谱智能巡检系统巡视发现缺陷

如对上述产品和解决方案感兴趣，请联系：

深圳航天科创实业有限公司 马经理 18810635251（微信同号）

WAPI 产业联盟成员单位名录

中国移动通信集团公司	弘浩明传科技股份有限公司	吉翁电子（深圳）有限公司
中国电信集团公司	京信通信技术（广州）有限公司	北京汇为永兴科技有限公司
中国联合网络通信集团有限公司	北京城市热点资讯有限公司	福建星网锐捷网络有限公司
国家密码管理局商用密码检测中心	优比无线技术（深圳）有限公司	北京新岸线移动多媒体技术有限公司
国家无线电监测中心检测中心	南京智达康无线通信科技股份有限公司	广东欧珀移动通信有限公司
北大方正集团有限公司	上海欣民通信技术有限公司	上海贝尔股份有限公司
西安西电捷通无线网络通信股份有限公司	福建三元达通讯股份有限公司	成都鼎桥通信技术有限公司
北京中电华大电子设计有限责任公司	新华三技术有限公司	飞天联合（北京）系统技术有限公司
北京六合万通微电子技术有限公司	北京傲天动联技术股份有限公司	中国电力科学研究院
广州杰赛科技股份有限公司	中兴通讯股份有限公司	锐迪科微电子（上海）有限公司
深圳市明华澳汉科技股份有限公司	武汉虹信通信技术有限责任公司	苏州汉明科技有限公司
无锡中太数据通信有限公司	广州市卓纪思网络科技有限公司	神州数码网络(北京)有限公司
青岛海尔科技有限公司	赛芯电子技术（上海）有限公司	北京必虎科技股份有限公司
海信集团有限公司	雷凌科技股份有限公司	北京市政务网络管理中心
联想（北京）有限公司	瑞晟微电子（苏州）有限公司	天津赞普科技股份有限公司
华为技术有限公司	联发博动科技（北京）有限公司	北京数字认证股份有限公司
大唐移动通信设备有限公司	四川天邑信息科技股份有限公司	上海连尚网络科技有限公司
北京朗波芯微技术有限公司	湖南城市热点无线通信有限公司	深圳市瑞科慧联科技有限公司
大唐微电子有限公司	珠海市魅族科技有限公司	深圳市信锐网科技术有限公司
上海鼎芯科技有限公司	深圳市雄脉科技有限公司	福建新大陆通信科技股份有限公司
北京天一集成科技有限公司	奥泰尔科技（深圳）有限公司	北京比邻科技有限公司
北京联信永益信息技术有限公司	北京网贝合创科技有限公司	天津市电子机电产品检测中心
深圳鑫金浪电子有限公司	网件（北京）网络技术有限公司	高通无线通信技术（中国）有限公司
深圳市普天宜通科技有限公司	上海市数字证书认证中心有限公司	中科开创（广州）智能科技发展有限公司
北京汉铭信通科技有限公司	北京创原天地科技有限公司	北京华信傲天网络技术有限公司
西安大唐电信有限公司	阿德利亚科技（北京）有限责任公司	南京博洛米通信技术有限公司
深圳共进电子股份有限公司	深圳市华讯方舟软件信息有限公司	广西新海通信科技有限公司
北京华安广通科技发展有限公司	迈创智慧供应链股份有限公司	上海麓慧科技有限公司
深圳国人通信有限公司	科通宽带技术(深圳)有限公司	深圳市智开科技有限公司
东蓝数码有限公司	邦讯技术股份有限公司	南方电网数字电网研究院有限公司
美国安移通网络公司北京代表处	惠州市宝丰信息科技有限公司	深圳航天科创实业有限公司
北京五龙电信技术公司	晨星软件研发（深圳）有限公司	南方电网深圳数字电网研究院有限公司
北京同耀通电科技有限公司	卓望数码技术（深圳）有限公司	广西电力线路器材厂有限责任公司
北京登合科技有限公司	迈普通信技术股份有限公司	广西通量能源技术有限公司
宇龙计算机通信科技（深圳）有限公司	北京汇通融业科技发展有限公司	
上海润欣科技有限公司	上海寰创通信科技有限公司	

【注：截至2021年8月，联盟正式成员已达106家，以加入联盟的时间先后排序。】

WAPI Alliance
产 | 业 | 联 | 盟



地 址：北京市海淀区知春路27号量子芯座1608室

邮 编：100191

电 话：010-82351181

传 真：010-82351181 ext. 1901

邮 箱：wapi@wapia.org

网 址：<http://www.wapia.org.cn>