工业互联网产业联盟
Alliance of Industrial Internet

工 业 互 联 网 产 业 联 盟 标 准

AII/009-2021

工业互联网 时间敏感网络 安全技术要求

Time Sensitive Network Security Technical Requirements for the Industrial Internet

工业互联网产业联盟

（2021 年 11 月 19 日发布）

声　　明

本报告所载的材料和信息，包括但不限于文本、图片、数据、观点、建议，不构成法律建议，也不应替代律师意见。本报告所有材料或内容的知识产权归工业互联网产业联盟所有（注明是引自其他方的内容除外），并受法律保护。如需转载，需联系本联盟并获得授权许可。未经授权许可，任何人不得将报告的全部或部分内容以发布、转载、汇编、转让、出售等方式使用，不得将报告的全部或部分内容通过网络方式传播，不得在任何公开场合使用报告内相关描述及相关数据图表。违反上述声明者，本联盟将追究其相关法律责任。

工业互联网产业联盟

联系电话：010-62305887

邮箱：aii@caict.ac.cn

目　　次

前　言

本标准是工业互联网时间敏感网络系列标准之一：
—工业互联网 时间敏感网络 交换机技术要求
—工业互联网 时间敏感网络 网关设备技术要求
—工业互联网 时间敏感网络 端设备技术要求
—工业互联网 时间敏感网络 交换机测试方法
—工业互联网时间敏感网络 运维管理技术要求
—工业互联网 时间敏感网络 安全技术要求
—工业互联网 时间敏感网络 可靠性要求
—工业互联网 时间敏感网络 流量模型规范
—工业互联网 时间敏感网络 管理设备技术要求

本标准是工业互联网 时间敏感网络安全技术要求，遵循 GB/T 1.1-2020 制定。
随着技术的发展，还将制定后续的相关标准。
本文件由工业互联网产业联盟提出并归口。

标准牵头单位：新华三技术有限公司
标准起草单位和主要起草人：

新华三技术有限公司：孙芳、涂蝉永、万晓兰、杨东红、吴晓佳

之江实验室：陈页、张建锋、许东阳、李振廷、邹涛、卢东辉

中国信息通信研究院：张恒升、段世惠、朱瑾瑜

中国移动通信有限公司研究院：郑师应

引　言

随着工业 4.0 时代的到来，时间敏感网络技术的产生，进一步促进了 IT 与 OT 融合发展，工厂环境更加开放，有线和无线接入方式增多，组网环境复杂和动态化。工业互联网时间敏感网络部署架构和时间敏感网络安全需求将逐步增加。

时间敏感网络安全将基于时间敏感网络部署架构基础上制定一套安全技术要求。将针对时间敏感网络部署架构中各网络层级制定安全技术要求。

本文件旨在指导各重点领域及相关单位进行时间敏感网络部署时，对各网络节点的时间敏感网络安全进行规划和设计，对时间敏感网络安全部署具有重要意义。

Alliance of Industrial Internet

工业互联网 时间敏感网络安全技术要求

1 范围

本标准规定了工业互联网中时间敏感网络安全技术要求。

本标准适用于工业互联网工控等领域中工业企业（以制造业为代表）内部网络中时间敏感网络的网络安全规划、设计与建设优化。

2 规范引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

YD/T 3489-2019 SDN网络安全能力要求

ITU-T X.1038 SDN网络安全要求和参考架构（Security requirements and reference architecture for software-defined networking）

IEEE Std 802.1Qcc-2018 IEEE 局域网和城域网标准 虚拟桥接城域网 修订：流量预留好的性能增强(IEEE Standard for Local and Metropolitan Area Networks ---Bridges on Bidged Network ---Amendment：Stream Reservation Protocol (SRP) Enhancements and Performance Improvements)

3 术语、定义和缩略语

3.1 术语和定义

下列术语和定义适用于本文件。

3.1.1

时间敏感网络 time-sensitive network

具有为业务流量提供有上限的确定时延传输能力的网络。

3.1.2

软件定义网络 software-defined networking

一种网络虚拟化的实现方式，通过将网络控制面与数据面分离开来，并提供开放编程接口，从而实现网络的灵活控制。

3.1.3

证书管理 certificate management

指负责生成、存储、分发、停用、撤销、归档和应用证书的统一安全策略。

3.1.4

认证 authentication

核实用户、程序或装置的身份，这常常是允许获取信息系统资源的前提条件。

标准引用自文件[NIST-SP-800-53] Appendix B

3.1.5

访问控制 access control
防止未授权使用资源，包括防止以未授权方式使用资源。
标准引用自文件[ITU-T X.800]3.3.1 章节

3.1.6

授权 authorization
授予用户、程序或装置某种权限。

3.1.7

公开密钥证书 public-key certificate(PKC)
用户的公开密钥，以及其他一些信息，利用发放它的认证机构的专用密钥，通过数字签名不可伪造地予以提供。
标准引用自文件[ITU-T X.509]3.3.46 章节

3.1.8

保密性 confidentiality
使信息不泄露给未授权的个人、实体或过程或者不使信息为其利用的特性。
标准引用自文件[ITU-T X.800]3.3.16 章节

3.1.9

数据完整性 data integrity
数据未被以未授权方式修改或破坏的特性。
标准引用自文件[ITU-T X.800]3.3.21 章节

3.1.10

密钥 key
控制加密与解密操作的符号系列
标准引用自文件[ITU-T X.800]3.3.32 章节

3.1.11

密钥管理 key management
依据安全策略生成、存储、分发、删除、存档和应用密钥。
标准引用自文件[ITU-T X.800]3.3.33 章节

3.1.12

威胁 threat
可能对系统或机构造成伤害的有害事件的潜在起因。
标准引用自文件[ISO/IEC 27000]2.45 章节

3.1.13

漏洞 vulnerability
可由威胁来源加以利用的信息系统、系统安全程序、内部控制或实施中存在的弱点。

标准引用自文件[NIST-SP-800-30] Appendix B

3.2 缩略语

下列缩略语适用于本文件。

API	应用程序编程接口	Application Programming Interface
CNC	中心网络控制器	Centralized Network Configuration
CUC	中心用户控制器	Centralized User Configuration
DDos	拒绝服务	Denial of Service
MAC	媒体接入控制	Media Access Control
TSN	时间敏感网络	Time-Sensitive Network
UNI	用户/网络配置信息	User/Network Configuration Information

4 概述

4.1 时间敏感网络架构

工业互联网领域下时间敏感网络架构参考 IEEE std 802.1Qcc-2018，建议采用集中式控制模型，由CUC、CNC、网管以及网络节点组成，如图 1 所示。具体内容如下：

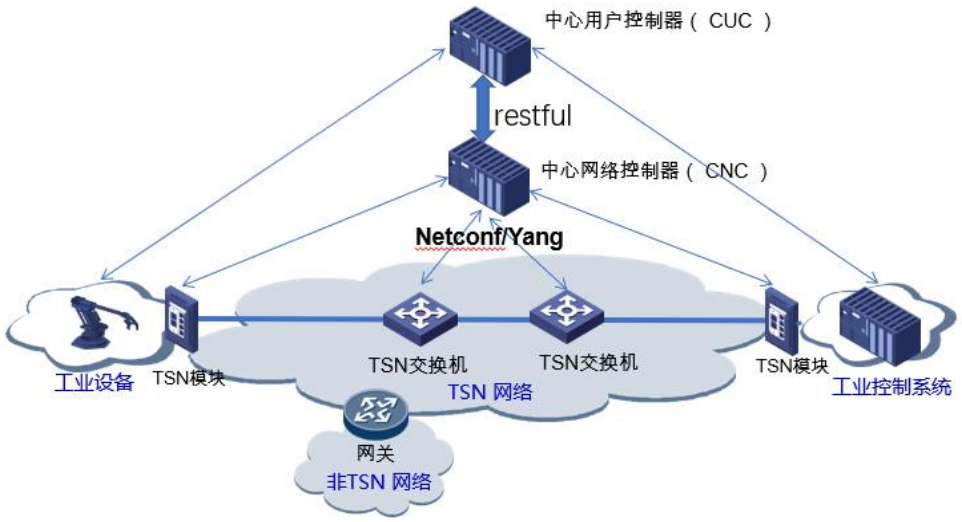

图 1 时间敏感网络架构图

a)时间敏感网络 CUC 节点，作为网络系统用户侧界面，用于管理工业应用系统并通过 UNI 接口(restful)向 CNC 提供端到端应用系统之间网络业务配置要求；

b)时间敏感网络 CNC 节点，通过南向接口（netconf/Yang）向网络节点下发相关配置；

c)时间敏感网络转发设备节点负责进行实际的报文转发，根据应用场景及网元在网络中的位置，将时间敏感网络转发设备分为网关、桥设备、端设备三种类型；

d)时间敏感网络的网管节点可以与 CNC 节点物理上合设，负责网络设备的故障监控及资源管理。

4.2 时间敏感网络安全逻辑框架

TSN 集中式控制模型与 SDN 技术架构类似，参考《YD/T 3489-2019 SDN 网络安全能力要求》、《ITU-T X.1038 SDN 网络安全要求和参考架构 Security requirements and reference architecture for software-defined networking》的规定，TSN 网络分为应用层、控制层和网络层三层架构。

TSN 网络安全威胁可分为两类：

一是基于传统网络面临的安全和威胁在 TSN 网络中也存在，如拒绝服务攻击、口令猜解、数据库漏洞利用等，但这些安全威胁的影响范围、重要程度等由于 TSN 的集中式控制模型而发生了变化。如，就拒绝服务而言，其对 TSN CNC 所造成的危害程度远远高于其对桥设备的危害；

二是 TSN 网络特有设备、协议和接口所带来的安全威胁，如 TSN CUC、时钟同步协议、资源预留协议、南北控制接口等自身安全漏洞造成的威胁。

TSN 网络每一层负责不同的功能以及对应不同的安全能力要求，如图 2 所示。

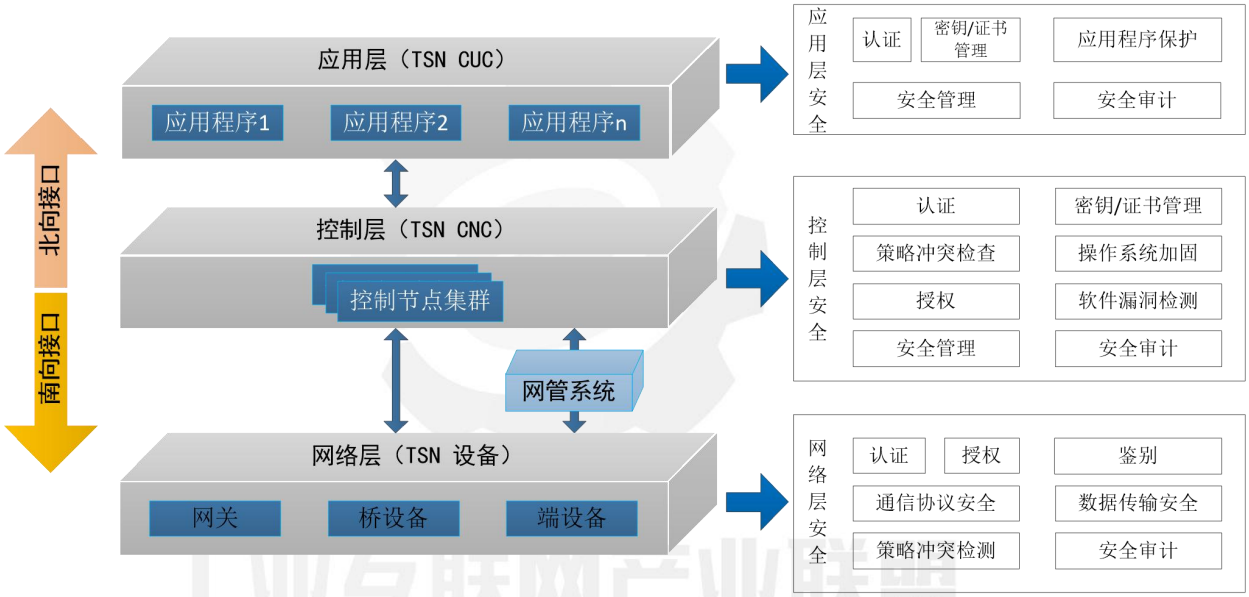

图 2 TSN 网络安全逻辑架构

应用层主要由用户控制器（TSN CUC）和不同的应用逻辑组成，通过控制层北向接口开放的API实现对网络资源的调配以及网络信息的获取，按需向用户提供网络能力

控制层主要由网络控制器（TSN CNC）、网管系统及相关控制软件组成，CNC通过南向接口向网络层转发节点下发策略和控制信息，通过北向接口向上层业务层开放底层网络资源和能力；网管系统则提供网络运维有关的能力，如设备、用户、日志的管理及网络状态的监控，并可以基于控制层提供的网络数据和资源信息

网络层主要由转发设备组成，承担数据信息在网络中的转发功能，主要包含时间敏感网络（TSN）转发节点及链路，同时网络层接受控制层通过南向接口下发的配置，并向控制层上报自身资源和状态。

5 时间敏感网络安全威胁

5.1 时间敏感网络应用层安全威胁

在 TSN 网络中，大部分功能由部署在应用层的各类 TSN 应用实现，如网络用户通过控制层北向接口开放的 API 实现对网络资源的调配以及网络信息的获取，按需向用户提供时间敏感网络的能力，因此攻击者对应用层的攻击会逐步影响到整个 TSN 网络，需要预先加以防范。

下述安全威胁会影响到 TSN 应用层：

5.1.1 欺骗

攻击者可以伪装成一个TSN CNC，骗取用户数据（用户密钥、证书等）、SLA、业务逻辑等信息，从而为进一步的攻击行为做准备。

5.1.2 抵赖

用户或管理员可以否认其曾经执行过的恶意网络策略，如将特定网络配置策略。

5.1.3 信息泄露

在获得用户认证信息后，攻击者可以伪装成一个合法用户，通过TSN应用向网络注入伪造信息流，以获取更多的网络数据。

5.1.4 应用程序自身漏洞

攻击者可以通过利用TSN应用程序自身漏洞（如代码缺陷等）获取相应的网络资源（例如：SLA，用户数据，业务逻辑等），从而为实施进一步攻击做准备。此外，第三方恶意应用可以伪装成为合法的应用程序来获取相应的网络资源。

5.2 时间敏感网络控制器层安全威胁

在 TSN 网络中，确保 TSN 的 CNC 安全至关重要，因为 CNC 是整个 TSN 网络的控制核心，一旦受到攻击，会直接危害整个 TSN 网络。

下述安全威胁会影响到 TSN 控制层：

5.2.1 流量转发策略冲突

新下发的流量转发策略可能与已有的策略发生冲突，导致预先部署的安全策略失效。

5.2.2 恶意流注入

攻击者可以通过劫持TSN应用，构造并发送一些恶意流量转发策略，实现数据窃听等恶意行为。

5.2.3 欺骗

攻击者可以通过伪装成管理员或TSN应用程序的手段，篡改CNC上的敏感数据（例如配置数据，用户数据等），获取网络拓扑结构、流量转发策略等信息，甚至完全控制CNC。通过CNC地址欺骗的方式，攻击者可以伪装CNC，从而获得整个TSN网络的控制权。攻击者甚至可以伪装成一个TSN桥设备，对目标TSN网络进行侦听。

5.2.4 抵赖

管理员或应用程序可以否认其曾经构造的恶意流量转发策略。

5.2.5 信息泄露

攻击者可以得到敏感的系统信息（例如配置数据，用户证书等），为进一步攻击做准备。

5.2.6 操作系统漏洞

由于CNC需要运行在操作系统上，因此操作系统的漏洞会导致CNC面临安全威胁。攻击者可以利用操作系统的漏洞，如默认密码，后门账户，开放端口、服务和协议等，去销毁或替换系统组件或整个系统，这样就会严重影响CNC。

5.2.7 软件漏洞

由于CNC是以软件的形式呈现给用户，因此软件自身的漏洞会导致CNC面临安全威胁。

5.3 时间敏感网络网络层安全威胁

下述安全威胁会影响到 TSN 网络层：

5.3.1 欺骗

攻击者可以冒充管理员或CNC去删除或修改TSN网络转发设备上的敏感数据（例如配置数据，流量转发策略表项等），或者获取流量转发策略等敏感信息。

5.3.2 协议攻击

攻击者利用协议存在的漏洞和安全脆弱性进行网络攻击，破坏正常的协议连接。

5.3.3 窃听

攻击者可以窃听TSN网络转发设备之间的数据流，从而得知有哪些数据流正在传输、哪些流量转发策略以及数据流的具体内容等。

5.3.4 恶意流量

攻击者发送某类恶意流量，有可能挤压另一个数据量带宽，导致流量延时或丢包。

5.3.5 流量转发策略表项溢出

由于TSN转发设备的流量策略表项和资源有限，使得其存在表项溢出的风险。攻击者可以不断的向TSN转发设备中注入流量转发策略，或利用泛洪攻击等方式，造成表项溢出。

5.3.6 抵赖

管理员或CNC可以否认其曾经执行过的错误配置。

6 时间敏感网络安全技术要求

6.1 应用层安全技术要求

应用层应具备的安全能力主要包括：对TSN CNC的认证、对用户和管理员的认证与授权、数据安全存储和传输、安全日志和审计以及抵御应用程序漏洞等。

6.1.1 认证

应用程序应对TSN控制器进行身份认证，以确保TSN控制器是真实的而不是一个伪造的恶意控制器。应支持的身份验证机制包括但不限于：基于共享密钥（pre-shared key）的身份认证机制、基于证书的身份认证机制。

6.1.2 密钥/证书管理

宜支持[ITU-T X.800]中定义的密钥管理和[IETF RFC4210]定义的证书管理。

6.1.3 应用程序保护

集中控制应用层宜部署相关攻击检测工具（如入侵检测系统、防火墙等），用来保护应用程序的安全稳定运行。攻击检测工具宜采用基于异常行为和基于数字签名的两种方式。

6.1.4 安全管理

安全管理应对用户进行审计、控制错误密码尝试次数、最小化系统平台需要的配置、强制执行操作系统的安全策略。安全管理宜对网络中的各类信息数据进行整合分析，用来支撑相应攻击检测等功能。

6.1.5 安全审计

应用层应提供日志和审计功能，记录用户曾经执行过的网络操作，应支持安全审计。

6.2 控制层安全技术要求

控制层应具备的安全能力，主要包括对管理员的安全认证和访问授权、对应用程序和端设备的安全认证、支持流量转发策略冲突防御和表项安全管理、安全日志和审计以及硬件故障发现与快速恢复等。

6.2.1 认证

TSN 控制器应对交换机、网关、端设备进行身份认证，以确保相应交换机、网关、端设备是真实的，不是伪造的。宜支持常用的身份认证机制，包括但不限于：基于用户名/密码的身份认证，基于预置密钥（pre-shared key）的身份验证，基于证书的身份验证。

6.2.2 密钥/证书管理

宜支持[ITU-T X.800]中定义的密钥管理和[IETF RFC4210]定义的证书管理。

6.2.3 策略冲突检查

TSN 控制器新生成的流量转发策略可能会与原有的策略相冲突，导致原有策略的失效。因此，TSN 控制器应对相应网络策略（插入/更新/删除流量转发策略）进行管理，从而避免策略冲突。

6.2.4 操作系统加固

操作系统加固能够最大程度消除安全风险，使操作系统更加安全。操作系统加固宜支持的操作包括但不限于：正确配置系统和网络组建，删除无用的文件，删除所有不必要的软件程序，更新补丁，格式化硬盘，至安装服务器必须的功能，禁用来宾账户，重命名管理员账户。

6.2.5 授权

TSN 应用程序和管理员访问 TSN 控制器时应遵守访问控制策略。宜支持的访问控制机制，包括但不限于：白名单/黑名单，访问控制列表（ACL），基于角色的访问控制（RBAC）。

6.2.6 软件漏洞检测

不应存在已公布的漏洞，或具备补救措施防范漏洞安全风险，不应存在恶意程序，不应存在未声明的功能和访问接口。

6.2.7 安全管理

安全管理是指对系统平台、资源的访问控制，避免非授权使用或修改相关安全策略。安全管理应支持对用户进行审计、控制错误密码尝试次数、最小化系统平台所需要的配置、强制执行操作系统的安全策略。安全管理宜支持对网络中的各类信息数据进行整合分析，用来支撑相应攻击检测等功能。

6.2.8 安全审计

控制层应提供日志和审计功能，记录控制器曾经执行过的操作，应支持安全审计。

6.3 网络层安全技术要求

网络层应具备的安全能力主要包括：对TSN CNC的认证、对管理员的认证与授权、数据安全存储和传输、安全流量控制以及安全日志和审计等。

6.3.1 认证

TSN 网络转发设备应支持对管理员、TSN CNC 进行身份认证，以确保相应管理员、CNC 是真实的，不是伪造的。

6.3.2 授权

TSN 网络转发设备应支持对管理员提供授权功能，以确保管理员访问设备时需要遵守访问控制策略。

6.3.3 鉴别

TSN 网络转发设备应支持对终端设备进行鉴别，至少支持如下机制之一：

a）基于网络标识的鉴别；

b）基于 MAC 地址的鉴别；

c）基于通信协议的鉴别；

d）基于通信端口的鉴别；

e）基于口令鉴别。

6.3.4 通信协议安全

TSN 网络转发设备应满足如下要求：

a）应满足通信协议健壮性要求，防范异常报文攻击。

b）应具备抵御常见重放类攻击的能力。

6.3.5 数据传输安全

TSN 网络转发设备应满足如下要求：

a）时间敏感网络应可以根据实际业务要求实现资源保护，划分相应的时间敏感网络域，并进行相应隔离。

b）能够根据应用需求灵活配置实时数据流与非实时数据流的带宽占比，合理控制网络中不同类型数据流量的大小，防止某类恶意流量对带宽的阻塞。

6.3.6 策略冲突检测

TSN 控制器新生成的流量转发策略可能会与原有的策略相冲突，导致原有策略的失效。因此，TSN 网络转发设备应支持对相应网络策略（插入/更新/删除流量转发策略）进行检测和管理，并将网络策略上送控制器，从而避免策略冲突。

6.3.7 安全审计

TSN 网络转发设备应提供日志和审计功能，记录设备的安全事件、异常操作，应支持安全审计。

参 考 文 献

[1] 2018-1367T-YD 工业互联网 时间敏感网络技术要求（报批中）.