ICS 35.040

L 80

中华人民共和国国家标准

GB/T XXXXX—XXXX

信息安全技术　基于信息流的关键信息基础设施边界确定方法

Information security technology — Method for critical information infrastructure boundary identification based on information flow

（征求意见稿）

（本稿完成日期：2019 年 4 月 21 日）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准按照GB/T 1.1—2009《标准化工作导则 第1部分：标准的结构和编写》给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由全国信息安全标准化技术委员会（SAC/TC260）提出并归口。

本标准主要起草单位：

本标准主要起草人：

引　言

认定关键信息基础设施，是开展关键信息基础设施安全保护工作的前提和基础，对于明确保护对象、实施重点保护具有重要作用。

本标准针对关键信息基础设施识别问题，描述了关键信息基础设施边界识别原理，规范了关键信息基础设施边界识别的流程、方法。《信息安全技术 关键信息基础设施网络安全保护要求》对关键信息基础设施安全防护进行了规范，《信息安全技术　关键信息基础设施安全检查评估指南》对关键信息基础设施安全检查进行了规范。

信息安全技术　基于信息流的关键信息基础设施边界确定方法

1　范围

本标准描述了关键信息基础设施组成结构和关键信息基础设施边界识别原理，给出了关键信息基础设施边界识别模型，规范了关键信息基础设施边界识别的流程、方法和要求，为关键信息基础设施边界识别工作提供一种方法性指南。

本标准适用于关键信息基础设施保护工作部门、关键信息基础设施运营者识别关键信息基础设施边界，明确保护对象，确定保护范围，进而实施重点保护。

2　规范性引用文件

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。

GB/T 25069　信息安全技术　术语

3　术语和定义

GB/T 25069 和 GB/T 31495.2—2015 中界定的以及下列术语和定义适用于本文件。

3.1

关键信息基础设施　critical information infrastructure

公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的网络设施、信息系统。

3.2

关键信息基础设施元素　critical information infrastructure component

对构成关键信息基础设施的网络设施、信息系统的统称。其中，网络设施是指连接通信信息网络（互联网、物联网、工控网、专用网等）的基础性网络设施，以及在上述网络中对信息数据进行发送、传输、控制等操作的网络设备；信息系统是指由计算机软硬件、数据、规章制度等组成的按照一定规则运行的功能单元。

3.3

关键信息基础设施边界　critical information infrastructure boundary

确定关键信息基础设施元素的分界线，用于将关键信息基础设施元素同其它信息基础设施区分开来，以明确关键信息基础设施保护对象和保护范围。

3.4

业务信息 business information

业务核心功能正常运行所必须的信息数据的统称。

3.5

业务信息流 business information flow

业务信息从产生到终止，在整个生命周期内的流动轨迹。

4 缩略语

下列缩略语适用于本文件。

CII：关键信息基础设施（Critical Information Infrastructure）

BI：业务信息（Business Information）

BIF：业务信息流（Business Information Flow）

OMS：停电管理系统（Outage Management System）

5 CII边界识别原理

5.1 CII存在条件

关键业务是CII存在的前提和基础，开展CII边界识别的目标是将支撑关键业务稳定、持续运行的网络设施、信息系统识别出来，实施一体化重点保护。存在CII的关键业务应符合下列两个必要条件：

a) 关键性条件

CII所支撑的关键业务一旦遭到破坏、丧失功能或者数据泄露可能严重危害国家安全、国计民生、公共利益。

b) 信息化条件

CII所支撑的关键业务高度依赖信息化运行，即一旦支撑关键业务运行的网络设施、信息系统遭受攻击会给关键业务的核心功能造成严重危害。

5.2 CII形态构成

CII在形态构成上是网络设施、信息系统或者是由多个网络设施、信息系统组成的集合，为关键业务提供信息化支撑，是关键业务的信息化组成部分。

5.3 CII支撑业务的方式

CII元素按照业务运行逻辑和功能划分，通过设计信息、存储信息、整合信息、删除信息等方式提高业务行为效率，保障业务自动化、智能化、高效运行，CII对业务的支撑方式具体表现为下列九种，或者是下列九种方式的组合：

a) 信息产生

是指根据业务需求，按照预设信息模式产生信息数据，使之能够有效地存储、流转等，满足业务各个应用环节的需求,又称信息起源或者信息设计。

b) 信息采集

是指根据业务需求，将设计好的信息数据收集起来的过程，又称信息获取。

c） 外部信息采集

是指根据业务自身的需求，收集除自身设计以外的信息数据。

d） 信息整合

是指把在不同信源的信息数据收集、整理、清洗，转换后加载到一个新的信源，为信息处理提供统一视图。

e） 信息处理

是指从大量的、可能是杂乱无章的、难以理解的信息数据中抽取并推导出对于某些特定的有价值、有意义的信息数据。在表现形式上可能是采集、存储、检索、加工和变换。

f） 信息呈现

是指按照业务预设功能，将信息起源阶段所要达到目标的最终展示。

g） 其它应用

是指将信息数据用于业务自身以为的其它用途。

h） 信息存储

是指将信息数据以某种格式记录在介质上。

i） 信息销毁

是指信息消亡的过程，分为两种，一种是可恢复删除，另外一种是不可恢复删除。

5.4 CII 边界识别模型

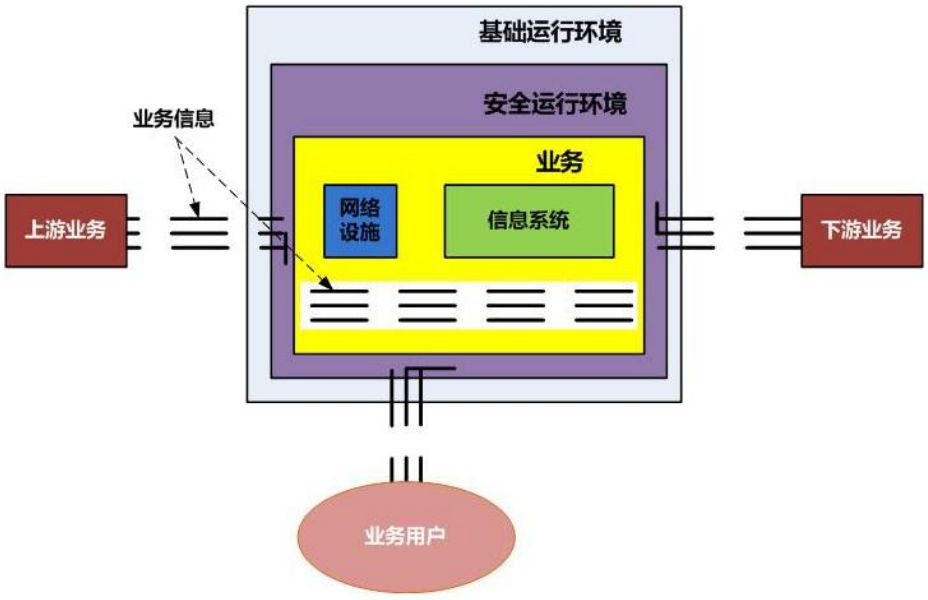

图1：CII边界识别模型

业务、网络设施、信息系统、业务信息、安全运行环境、基础运行环境，是识别CII边界需要考虑的六个方面。

识别CII边界，首先要识别关键业务，关键业务是核心要素，其它要素都是围绕着关键业务产生的：即网络设施、信息系统是关键业务正常运行所必须的信息化部分，与业务是信息化支撑关系；业务信息是关键业务正常运行所必须的数据资源，同时也是网络设施、信息系统实现对关键业务信息化支撑的纽带和桥梁，网络设施、信息系统按照业务运行逻辑和功能划分对业务信息进行处理，包括设计、存储、整合、删除等操作，实现了对关键业务核心功能的信息化支撑；安全运行环境主要包括安全设备、控制

措施、安全策略、规章制度等，用于保障关键业务的信息安全；基础运行环境为关键业务正常运行提供电力、空调等基础条件。

基于上述概念，图1给出了CII边界识别模型。网络设施、信息系统是CII元素的候选对象，其中一旦遭到攻击、丧失功能或者数据泄露会严重影响关键业务稳定、持续运行的网络设施、信息系统纳入CII保护范围。

因此，CII边界识别的基本原理可以概括为，关键业务核心功能安全运行所必须的信息数据，从产生到终止所流经的重要网络设施、信息系统组成了支撑该业务的CII。

6 CII 边界识别要求

6.1 基本原则

CII边界识别的核心是将保障关键业务稳定、持续运行必不可少的网络设施、信息系统同CII运营者一般的信息基础设施区分开来，明确保护对象和保护范围，为制定CII保护措施提供科学依据。CII边界识别应遵循下列整体原则：

a） 业务安全原则

CII边界识别应以保障关键业务安全运行为目标，将支撑关键业务稳定、持续运行必不可少的网络设施、信息系统识别出来。

b） 重点保护原则

CII边界识别应突出重点，聚焦一旦遭到破坏、丧失功能或者数据泄露会给关键业务的核心功能造成严重危害的网络设施、信息系统，严格控制范围。

c） 边界清晰原则

CII边界识别应以关键业务为基本单元，将支撑同一关键业务运行的网络设施、信息系统认定为同一个CII，且每一个CII都应有明确的运营者。

d） 一体化防护原则

对于跨不同运营者的关键业务，开展CII边界识别应充分考虑对上下游业务的安全影响，从一体化防护原则的角度出发识别CII边界。

6.2 实施要求

行业领域差异性大、专业强，为充分反映行业领域网络安全工作特点，CII边界识别工作应采用国家保护部门、行业领域专家和CII运营者共同参与的方式，确保识别结果的准确性、科学性和权威性。具体实施要求如下：

a） CII 边界识别工作应在国家网信部门统一组织协调下实施。

b） 实施 CII 边界识别活动不应影响关键业务的正常运行，避免在边界识别过程中出现重大网络安全事件。

c） 应制定详细的网络安全应急预案，确保在 CII 边界识别过程中出现的重大网络安全事件得到快速、有效的处置。

6.3 保密要求

a） CII 边界信息涉及关键业务的稳定、持续运行，一旦泄露可能影响国家安全、国计民生、公共利益，任何组织和个人，不得将收集到的 CII 边界信息向任何非授权方透露。

b) CII 边界识别从业人员应获得国家有关部门的授权，并在边界识别过程中遵循国家法律法规有关规定。

c) CII 边界识别工作由第三方机构开展实施的，委托方、实施方和 CII 运营者应制定详细保密方案，并签订保密合同。

6.4 识别周期

CII边界识别应采用动态工作方式，及时更新CII边界信息，确保CII边界信息的时效性。CII边界识别周期应满足如下要求：

a) 每年应至少开展一次边界识别工作。

b) 当 CII 运营者的组织结构、业务架构、从属关系等发生重大调整时，应在调整结后及时实施边界识别工作。

7 CII 边界识别流程

CII边界识别流程见图2。

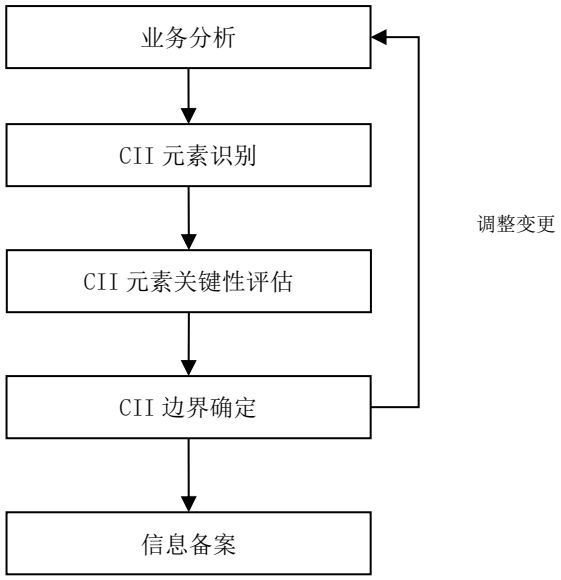

图2：CII边界识别流程

CII边界识别流程主要包括业务分析、CII元素识别、CII元素关键性评估、CII边界确定和信息备案5个部分，适用情况说明如下：

a) CII 边界识别流程适用于关键业务已经明确的情形，对于关键业务尚没有确定的情况不适用于此流程。

b) 业务发生重大变化、或者新运行的业务，运营者应首先上报行业主管部门，待行业主管部门评估认定后再按照此流程开展边界识别工作；

c) 在业务设计、建设等阶段就被行业主管部门认定为是关键业务的，待业务正式运行后可以按照此流程开展 CII 边界识别工作。

8 业务分析

8.1 业务分析流程

业务分析包括业务识别、业务梳理、业务特征识别和业务信息化描述，明确关键业务以及关键业务信息化运行情况，是识别 CII 元素的基础工作，如图 3 所示。

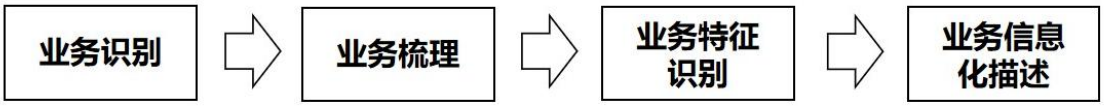

图 3：业务分析流程

8.2 业务识别

业务识别是指将 CII 运营者所运行的关键业务识别出来的活动。关键业务由行业主管部门认定，组织开展 CII 边界识别工作应以行业主管部门认定的关键业务为基准。

8.3 业务梳理

根据关键业务所在的行业领域特点，调查了解关键业务运行情况，形成关键业务基本情况描述文件。一个典型的关键业务基本情况描述文件应包含以下内容：

a) 主管机构；
b) 运营者基本情况；
c) 业务开展范围；
d) 业务服务对象；
e) 上下游业务情况。

8.4 业务特征识别

根据业务基本情况，调查了解业务运营的组织架构、管理框架、管理策略、规章制度、地理位置、岗位设置和岗位职责等方面信息，梳理业务运行逻辑，识别业务核心功能，在此基础上形成业务特征描述文件。一个典型的业务特征描述文件应包含以下内容：

a) 业务运行架构；
b) 资产分布情况；
c) 业务核心功能介绍；
d) 业务关键性介绍。

8.5 业务信息化描述

根据业务基本情况和业务特征，调查了解业务的信息化建设、信息化管理、信息化运维等方面信息，并在此基础上形成业务信息化描述文件。一个典型的业务信息化描述文件应包含以下内容：

a) 支撑业务信息运行的网络拓扑结构；
b) 网络设施、信息系统部署情况；
c) 设备资产清单。

9 CII 元素识别

9.1 CII 元素识别流程

业务分析包括BI识别、BIF识别和CII元素归集，梳理支撑关键业务稳定、持续运行的网络设施、信息系统，确定CII元素候选清单，是开展CII元素关键性评估的准备工作，如图4所示。

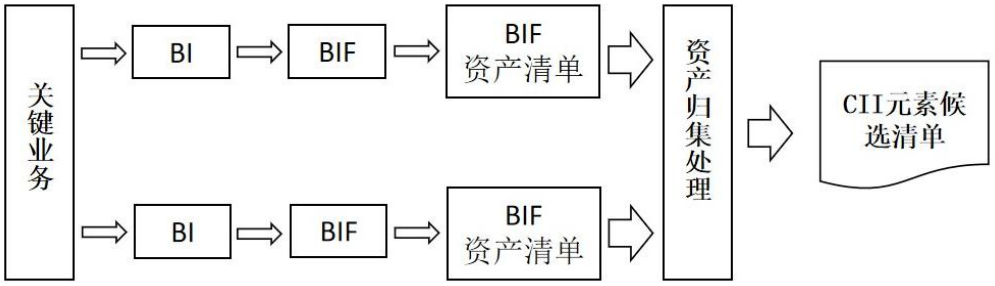

图4：CII元素识别流程

9.2 BI 识别

根据业务基本情况、业务特征和业务信息化运行情况，梳理关键业务稳定、持续运行必不可少的BI，并在此基础上形成BI描述文件。一个典型的BI描述文件应包含以下内容：

a) BI 类别介绍；

b) BI 用途介绍。

9.3 BIF 识别

梳理BI从产生到终止的全生命周期内的流动轨迹，即BIF。调查了解BIF上的网络设施、信息系统部署详情，并在此基础上形成BIF描述文件。一个典型的BIF描述文件应包含以下内容：

a) BI 生命周期介绍；

b) BIF 对应的网络设施、信息系统部署详情。

9.4 CII 元素归集

对所有BIF上的网络设施、信息系统进行归集处理，得到支撑该关键业务的网络设施、信息系统清单，即CII元素候选清单，并在此基础之上形成CII元素候选清单描述文件。一个典型的CII元素候选清单描述文件应包含以下内容：

a) 候选 CII 元素网络拓扑图；

b) 候选 CII 元素部署详情；

c) 候选 CII 元素对业务核心功能支撑情况说明；

d) 设备资产清单。

10 CII 元素关键性评估

10.1 评估方法

CII元素关键性评估是指评估CII候选元素一旦遭到破坏、丧失功能或者数据泄露对关键业务稳定、持续运行所造成的影响。评估指标包括但不限于业务可用性、业务完整性和数据机密性，评估结果为关键的CII后续元素纳入CII保护范围。

10.2 评估指标

a） 业务可用性

业务可用性遭到破坏是指CII遭到破坏后丧失基本功能，完全无法对业务进行信息化支撑。比如，铁路的信号控制系统遭到破坏以后，无法对列车发出预警或者停车信号；灾情预警系统遭到破坏后，无法提供险情预警数据，也无法发出控制指令；云服务出现故障，拒绝任何形式的访问请求等。

b） 业务完整性

业务完整性遭到破坏是指CII遭到破坏虽然没有完全丧失对业务的信息化支撑，但是业务功能受到影响，比如信息交互速率远低于预设水平、某子功能完全缺失等。例如，运营商的数据管道业务是按照既定速率将业务交付的信息从发送端提供给接收端，当支撑上述业务的CII受到攻击以后，这种信息交互速率就会降低；网络直播业务是在客户端和服务器之间传输信息（接收用户请求和将服务器上的视频信息推送给客户端），如果支撑上述功能的CII遭到攻击后，信息传输速率就会降低，表现为用户提交请求缓慢或者视频播放停顿；铁路购票系统具有现场购票、网络购票和电话购票三种功能，支撑网络购票的CII遭到攻击后，网上购票功能可能会完全丧失或者购票缓慢等。

c） 数据机密性

数据机密性遭到破坏是指CII遭到攻击后基本功能被篡改，对其所支撑的业务提供错误信息，或者将业务信息泄露出去。比如，电力控制系统是保障电力调度安全，一旦遭到攻击后会对供电系统发出错误指令；导航系统为用户提供准确位置信息，受到攻击后会提供错误位置信息；数据存储业务是云的一个重要功能，正常情况下只与授权用户之间进行信息交互，如果受到攻击可能会将信息提供给非法用户，即发生数据泄露。

10.3 评估流程

CII元素关键性评估流程如图5所示。

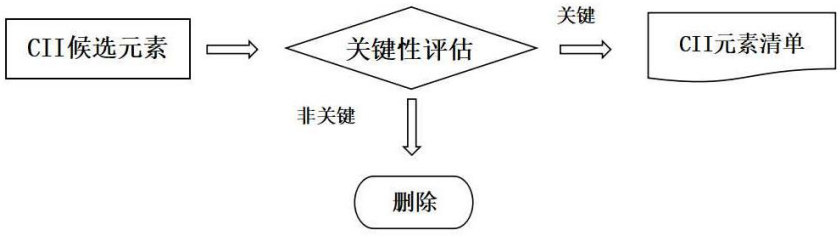

图5：CII元素关键性评估流程

根据CII元素关键性评估表，如表一所示，对CII候选元素进行关键性评估，具体流程说明说下：

a） 针对每一个 CII 候选元素，分析其一旦遭到破坏、丧失功能或者数据泄露对业务可用性、业务完整性和数据机密性所造成的影响；

b） 对任一评价指标造成影响的 CII 候选元素其关键性评估结果应为关键；对所有评价指标都无影响的 CII 候选元素其关键性评估结果应为非关键；

c） 将评估结果为关键的 CII 候选元素纳入 CII 元素清单。

表一 CII 元素关键性评估表

序号	评估对象	评估指标		
		业务可用性	业务完整性	数据机密性
1	网络设施	影响/否	影响/否	影响/否
2	信息系统	影响/否	影响/否	影响/否

11 CII 边界确定

11.1 目标

根据CII元素，确定CII边界，并将CII边界文档化，形成一套指导开展CII保护的文件。

11.2 CII 边界描述

根据识别出的CII元素形成CII边界总体描述文件，一个典型的CII边界总体描述文件应包含以下内容：

a) 业务基本情况描述；
b) 业务特征描述；
c) 业务关键性描述；
d) 业务信息化描述；
e) CII 元素描述；
f) CII 元素关键性评估说明；
g) CII 元素网络拓扑图；
h) CII 元素部署详情；
i) CII 元素资产清单。

12 信息备案

12.1 备案要求

CII 边界实施方应记录 CII 边界识别过程，编制 CII 边界识别认定报告，形成内部正式文件或向边界实施发起方报备。

12.2 备案内容

a) 运营者信息
包括运营者名称、统一社会代码、运营者性质、主要负责人信息、网络安全分管负责人信息。

b) 专门网络安全管理机构信息
包括机构名称、机构负责人、联系方式。

c) 行业领域说明
所属行业信息情况说明。

d） 关键业务说明

CII 所支撑、承载的业务情况介绍。

e） CII 清单和边界说明

边界识别过程说明、边界描述和 CII 目录清单。

附 录 A

（规范性附录）

关键信息基础设施边界信息登记表

<table>
<tr><td>01 运营者名称</td><td colspan="4"></td></tr>
<tr><td>02 统一社会信用代码</td><td colspan="4"></td></tr>
<tr><td>03 单位地址</td><td colspan="4">_____省（自治区、直辖市）_____市（区、地、州、盟）
_____县（区、市、旗）</td></tr>
<tr><td>04 单位性质</td><td colspan="4">01 党政机关　　02 事业单位　　03 国有企业
04 私营企业　　05 外资企业　　06 合资企业</td></tr>
<tr><td rowspan="3">05 主要负责人</td><td>01 姓名</td><td></td><td>02 职务</td><td></td></tr>
<tr><td>03 国籍</td><td></td><td>04 联系方式</td><td>01 座机：_____</td></tr>
<tr><td colspan="2"></td><td></td><td>02 手机：_____</td></tr>
<tr><td rowspan="3">06 分管网络安全负责人</td><td>01 姓名</td><td></td><td>02 职务</td><td></td></tr>
<tr><td>03 国籍</td><td></td><td>04 联系方式</td><td>01 座机：_____</td></tr>
<tr><td colspan="2"></td><td></td><td>02 手机：_____</td></tr>
<tr><td rowspan="3">07 专门网络安全管理机构</td><td colspan="4">01 机构名称：_____</td></tr>
<tr><td>02 机构负责人</td><td colspan="3">01 姓名：_____
02 办公电话：_____手机：_____
03 国籍：_____</td></tr>
<tr><td>03 联系人</td><td colspan="3">01 姓名：_____
02 办公电话：_____手机：_____
03 国籍：_____</td></tr>
<tr><td rowspan="8">08 行业领域</td><td>01 公共通信和信息服务</td><td colspan="3">01 电信　　02 互联网　　03 广播电视
04 卫星导航　　05 其它：_____</td></tr>
<tr><td>02 能源</td><td colspan="3">01 电力　　02 石油天然气　　03 石化
04 其它：_____</td></tr>
<tr><td>03 交通</td><td colspan="3">01 铁路　　02 公路　　03 水运
04 民航　　05 邮政　　06 城市轨道交通
04 其它：_____</td></tr>
<tr><td>04 水利</td><td colspan="3"></td></tr>
<tr><td>05 金融</td><td colspan="3">01 银行　　02 证券　　03 保险
04 其它：_____</td></tr>
<tr><td>06 公共服务</td><td colspan="3">01 教育　　02 卫生　　03 社会保障
04 市政服务　　05 其它：_____</td></tr>
<tr><td>07 电子政务</td><td colspan="3"></td></tr>
<tr><td>08 国防科技工业</td><td colspan="3"></td></tr>
<tr><td>09 关键业务简介</td><td></td><td colspan="3"></td></tr>
</table>

10 关键信息基础设施清单	序号	网络设施、信息系统名称
	01	
	02	
	……	

附 录 B

（参考性附录）

CII 边界识别示例

以电网为例，介绍 CII 边界识别活动，所示内容皆为去敏和去秘后的部分数据，只为说明 CII 边界识别方法，不代表真实数据。

一、业务分析

1、业务识别

电网运行稳态监视与控制是电网安全运行的重要保障，负责监测电力生产、电力传输、电力配送环节的运行态势，及时处理发现的安全隐患，一旦遭受网络攻击，会给整个电力系统的稳定运行造成严重影响。

2、业务梳理

电网运行稳态监视与控制业务分为省、市两级，分别由省级电力调控中心和市级电力调控中心负责运营，主管机构是省电力总公司。

省级电网运行稳态监视与控制业务主要负责管内 220kV 及以上电厂、变电站及部分 110kV 电厂、变电站稳态监测与控制，并将信息及时与管内各供电局共享；市级电网运行稳态监视与控制业务主要负责管内部分 110kV 电厂、变电站及 35kV 以上电厂、变电站稳态监测与控制，并将所管区域内的信息数据上送到省级电力调控中心，整个业务运行框架如图 5 所示。

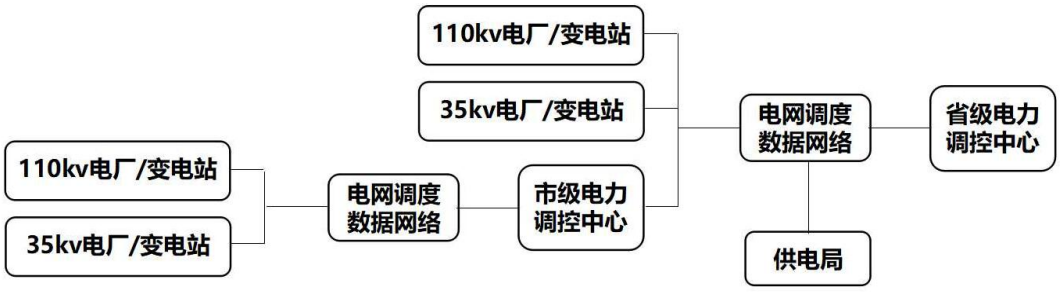

图5：电网运行稳态监视与控制业务运行架构

3、业务特征识别

电网运行稳态监视与控制业务主要负责调管范围内的电网运行态势监测和事故分析，控制开关刀闸、投切电容器、调节发电机组输出功率，确保机组总输出与用电总负荷实时平衡，保证电网电压质量合格，是整个电网安全运行的基础和核心保障。

4、业务信息化描述

部署在各电厂、变电站的监控系统和测控装置将各电厂、变电站运行态势信息通过电网调度数据网络自动上送给各级电力调控中心，最后数据归集到省级电力调控中心，网络拓扑如图 6 所示。

省级电力调控中心利用电网稳态监视与控制平台对收集到的电网运行态势数据实时智能化处理，实现对整个电网运行态势的感知。

电网稳态监视与控制平台在电网运行态势的基础之上，结合其他外部数据，比如风功率预测系统、OMS 等上报的数据，做出精准判断，并通过调度主站系统、智能远动子站系统、厂房子站系统将调控、调度指令下发给部署在各发电厂、变电站的监控系统和测控装置。

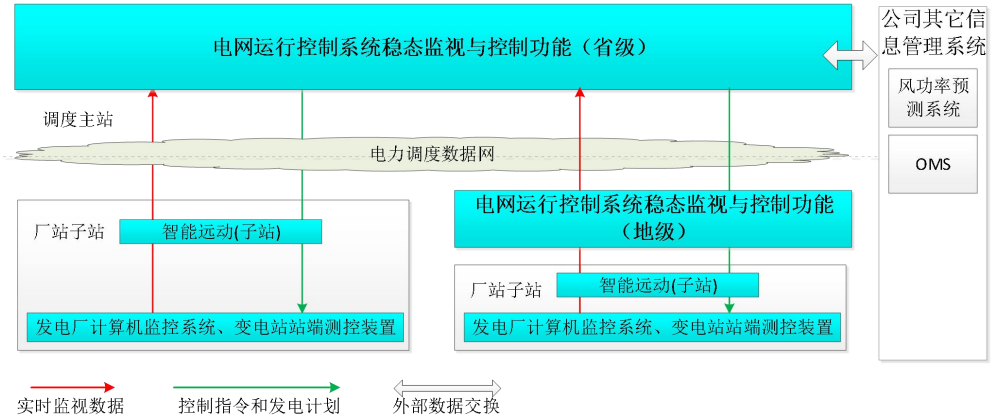

图6：电网运行稳态监视与控制网络拓扑结构

二、CII 元素梳理

1、 BI 识别

1.1 BI 类别

电网运行稳态监视与控制平台处理的主要信息数据分为三大类，一是电网运行态势信息；二是控制指令信息；三是共享信息。通过对电网运行态势信息的获取和处理，实现了对整个电网运行态势的实时感知，为下发控制指令提供决策依据。通过共享信息将电网实时运行态势共享给管内供电局，为供电局制定行业发展政策提供依据。

1.2 BI 功能

电网运行态势信息主要类别和功能如下：

a) 电能量计量信息主要用于监测实时用电量，为电力调度提供依据。

b) 继电保护信息主要实现对供电安全装置的运行状态、动作行为进行监测，在电网故障时则进行快速的故障分析。

c) 相量测量信息和行波测距信息主要用于对故障地点进行定位。

d) 天气、水纹自然数据，用于辅助下发控制指令。

控制指令信息主要类别和功能如下：

e) 控制指令，用于开合刀闸、投切电容器。

f) 发电计划指令，用于控制各发电机组的发电量。

共享信息主要类别和功能如下：

g) 电网运行态势信息，用于各供电局实时掌握用电量，为制定行业发展规划提供依据。

2、BIF 识别

2.1 BI 生命周期

a） 数据起源环节

电网运行稳态监视与控制平台的数据起源主要是由部署在各电厂、变电站和电网调度数据网络上的数据采集器产生的。

b） 数据收集环节

电网运行稳态监视与控制平台的数据收集主要是指将部署在各电厂、变电站和电网调度数据网络上的数据采集器将产生的数据收集起来的过程，该过程主要由相应的数据处理系统完成的。

c） 外部数据汇入环节

电网运行稳态监视与控制平台的外部数据汇入环节主要是天气、水纹等自然信息数据，主要由电网运行稳态监视与控制平台的数据中心完成。

d） 数据汇集环节

电网调度数据网络将分布在各监测点的数据汇集到片区电网运行稳态监视与控制平台的数据中心，或者电网运行稳态监视与控制平台的数据中心。

e） 存储环节

电网运行态势数据都存在片区电网运行稳态监视与控制平台的数据中心，或者电网运行稳态监视与控制平台的数据中心，并保障数据安全。

f） 数据处理环节

电网运行态势数据主要由电网运行稳态监视与控制平台的数据中心处理完成的。

g） 呈现环节

按照电网运行稳态监视与控制平台预设功能，最终将整个电网运行态势情况实时显示出来。

h） 其它应用

电网运行稳态监视与控制平台将电网运行态势信息共享给管内各供电局。

i） 数据删除

电网运行稳态监视与控制平台只存储一定周期内的电网运行数据，过期数据会定期删除。

2.2 BIF 资产清单

a） 电能量计量信息

电能量数据采集器、电能量数据处理系统、电能量纵向互联交换机、纵向加密装置、电力调度数据网、电网综合数据网、SAN 交换机、数据中心、大屏显示与控制系统。

b） 继电保护信息

继电数据采集器、采集服务器、电力调度数据网、电网综合数据网、SAN 交换机、数据中心、大屏显示与控制系统。

c） 相量测量信息

相量数据采集器、电力调度数据网、电网综合数据网、SAN 交换机、数据中心、大屏显示与控制系统。

d） 行波测距信息

行波数据采集器、电力调度数据网、电网综合数据网、SAN 交换机、数据中心、大屏显示与控制系统。

e） 天气、水纹信息

数据采集服务器、正反向隔离装置、电网综合数据网、大屏显示与控制系统。

f） 控制指令，

电网运行控制系统、电力调度数据网、纵向互联交换机、发电厂/变电站端远动装置、发电厂计算机端监控系统、变电站测控装置。

g） 发电计划指令

电网运行控制系统、电力调度数据网、纵向互联交换机、发电厂/变电站端远动装置、发电厂计算机端监控系统、变电站测控装置。

h） 共享信息

数据中心、WEB 系统、电网运行控制系统暂态监视与保信系统。

3、CII 元素归集

对梳理出的资产去重、合并、归集得到支撑电网运行稳态监视与控制的 CII 元素候选清单如下：

数据采集服务器、行波数据采集器、继电数据采集器、采集服务器、电能量数据采集器、电能量数据处理系统、电网运行控制系统、电能量纵向互联交换机、发电厂/变电站端远动装置、发电厂计算机端监控系统、变电站测控装置、纵向加密装置、正反向隔离装置、电力调度数据网、纵向互联交换机、电网综合数据网、SAN 交换机、WEB 系统、电网运行控制系统暂态监视与保信系统、数据中心、大屏显示与控制系统、电网运行控制系统。

三、CII 元素关键性评估

对梳理出的 CII 候选元素进行关键性评估，评估结果如表二所示。

表二 CII 元素关键性评估

序号	涉及信息系统和设备	评估结果（是/否关键）	边界范围（是/否）
终端设施	数据采集服务器	是	是
	行波数据采集器	否	否
	继电数据采集器	是	是
	电能量数据采集器	是	是
	电能量数据处理系统	是	是
	发电厂/变电站端远动装置	是	是
	发电厂计算机端监控系统	是	是
	变电站测控装置	是	是
	纵向加密装置	是	是
	正反向隔离装置	是	是
传输系统	电力调度数据网	是	是
	纵向互联交换机	是	是
	电网综合数据网	是	是
	SAN 交换机	是	是
后台系统	电网运行控制系统	是	是
	电网运行控制系统暂态监视与保信系统	是	是
	数据中心	是	是

访问端	大屏显示与控制系统	是	是
	WEB 系统	是	是

四、CII 边界确定

支撑电网运行稳态监视与控制业务的 CII 元素网络拓扑结构如图 7 所示。

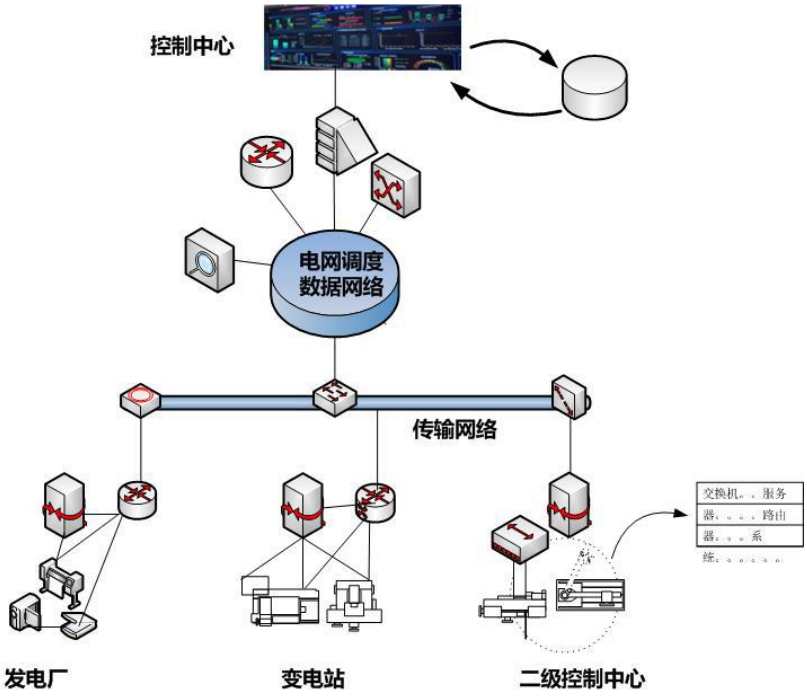

图7：CII（电网运行稳态监视与控制）元素网络拓扑结构

五、信息备案

a） 运营者信息

包括运营者名称、统一社会代码、运营者性质、主要负责人信息、网络安全分管负责人信息。

b） 专门网络安全管理机构信息

包括机构名称、机构负责人、联系方式。

c） 行业领域说明

电网运行稳态监视与控制业务属于“能源类”的“电力”。

d） 关键业务说明

电网运行稳态监视与控制平台主要监控 XXXX 家发电厂、变电站，涉及用电户 XXXX 家，一旦击会.....

e） 网络设施、信息系统目录

组成该 CII 的网络设施、信息系统清单。

参 考 文 献

[1] GB/T 22080—2016 信息技术 安全技术 信息安全管理体系要求
[2] GB/T 22239—2008 信息安全技术 信息安全等级保护基本要求
[3] GB/T 25069—2010 信息安全技术 术语
[4] GB/T 31496—2015 信息技术 安全技术 信息安全管理体系实施指南
[5] 中华人民共和国网络安全法，中华人民共和国全国人民代表大会常务委员会
[6] 国务院关于大力促进信息化发展和切实保障信息安全的若干意见，国发〔2012〕23号
[7] 关于加强国家网络安全标准化工作的若干意见，中网办发文〔2016〕5号
[8] ISO/IEC 25024:2015 Systems and software engineering - Systems and software Quality Requirements and Evaluation (SQuaRE) - Measurement of data quality