台州高速收费系统
路段级网络安全态势感知平台

建

设

方

案

浙江省交通规划设计研究院有限公司

2020 年 9 月

台州高速收费系统态势感知平台建设方案

一、项目概述

1.1.项目概况

交通运输部路网监测与应急处置中心于 2019 年 10 月下发了《收费公路联网收费系统网络安全态势感知平台体系建设方案》，指导全国各省份建设省级网络安全态势感知平台并与部平台实现对接。

为进一步满足交通运输部路网监测与应急处置中心网络安全态势感知平台建设要求，同时推进浙江省全省高速公路联网收费系统网络安全态势感知体系建设，浙江省公路与运输管理中心于 2020 年 9 月 3 日下发《浙江省收费公路联网收费系统网络安全态势感知平台体系建设方案》，要求本省各高速公路经营单位依照《浙江省高速公路联网收费系统网络安全态势感知平台体系建设方案》完成本级态势感知平台建设，并实现与省中心态势感知平台对接。

1.2.建设依据

- 《中华人民共和国网络安全法》
- 《信息安全技术网络安全等级保护基本要求》（GB/T 22239-2019）
- 《交通运输运输部关于印发〈联网收费系统省域系统并网接入网络安全基本技术要求〉的通知》（交科技函〔2019〕338 号）
- 《交通运输运输部办公厅关于印发〈收费公路联网收费系统网络安全信息通报工作规范（试行）〉的通知》（交办科技函〔2019〕950 号）
- 《收费公路联网收费系统网络安全态势感知平台体系建设方案》（交通运输部路网监测与应急处置中心 2019 年 10 月）
- 《关于推进全省高速公路联网收费系统网络安全态势感知平台建设的通知》（浙江省公路与运输管理中心-2020 年 9 月 3 日）

1.3.建设目标

2020 年 11 月底前，完成本路段系统态势感知平台建设，搭建起覆盖路段中心系统、收费站系统、及 ETC 门架系统的安全数据收集能力，本路段平台在 2020 年底前实现与省态势感知平台的对接。

二、需求分析

2.1.现状分析

黄岩管理中心（台州收费站）负责管理台州高速路段区域内高速公路联网收费系统的运行和建设，目前下属有 4 个收费站和 20 个 ETC 门架系统，现有收费系统内建设有较为完善的网络安全防护体系，并已达到部省相关文件的要求。

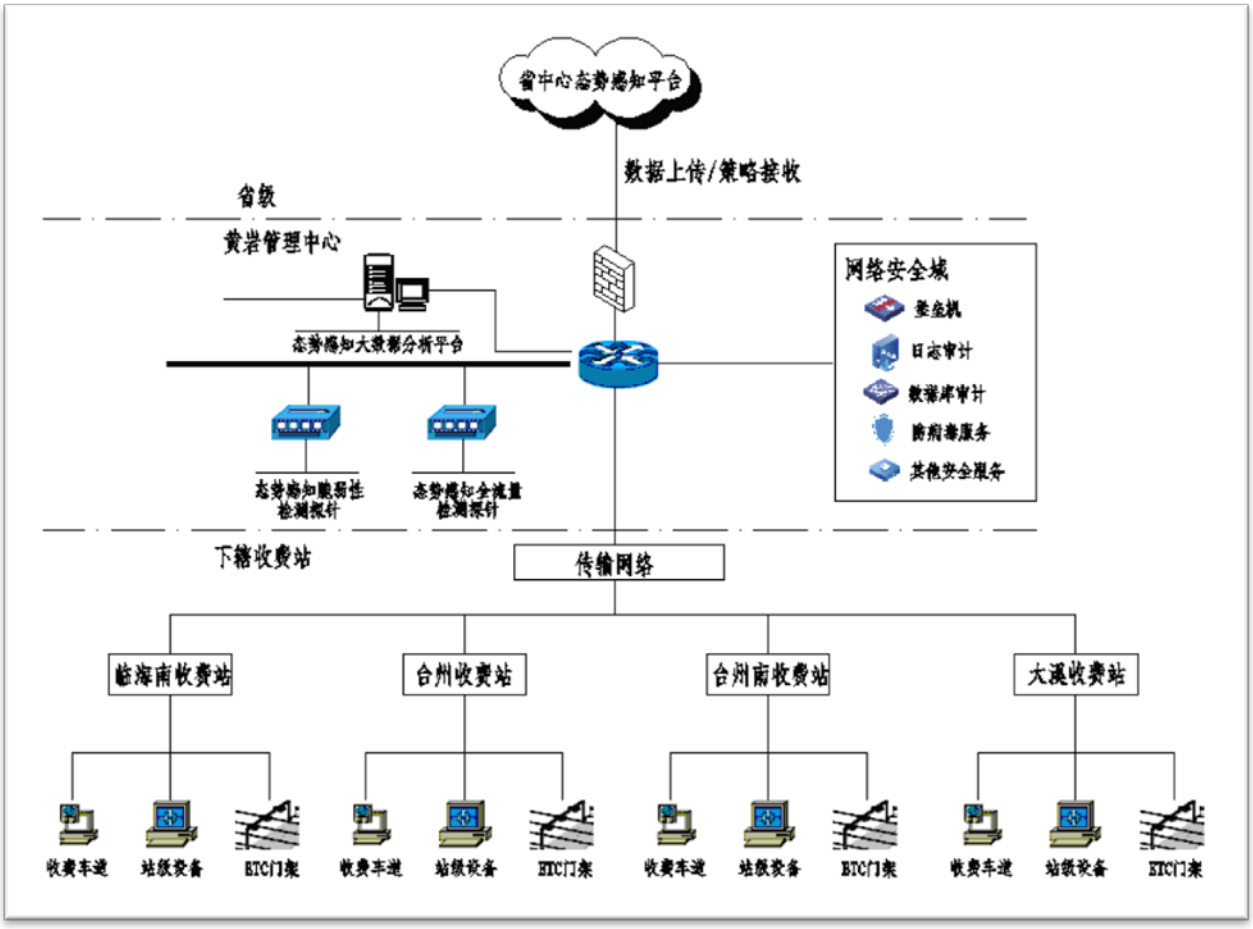
2.2 需求分析

根据部省对收费系统网络安全体系的建设安排，建设本路段的网络安全态势感知平台，平台按照“流量+日志”分析的方式对本路段的收费系统网络就行态势感知和预警分析，在与省平台对接后上传本路段的相关安全信息并接收省级态势感知平台下发的各类指令。

三、总体设计

3.1.总体架构

浙江省高速公路收费联网系统态势感知平台采用两级架构，第一级是省态势感知平台，第二级为区域/路段中心级态势感知平台，如下图所示：



本路段态势感知平台架构图

3.2.建设内容

根据部省相关文件的内容，本路段态势感知平台的建设采用“分析平台+安全探针”的方式，包括以下两部分内容：

1）态势感知数据分析平台；

2）安全探针；

四、建设方案

4.4.1.部署方式

台州高速现有收费系统包含 1 个分中心、4 个收费站和 20 套 ETC 门架系统，分中心、收费站和 ETC 门架系统目前网络全部联通，可在各节点访问整个网络，收费系统所

有流量均通过黄岩上传至省中心，本次设计在黄岩分中心内设置 1 套路段级态势感知数据分析平台、1 套态势感知全流量检测探针和 1 套态势感知脆弱性检测探针。

根据台州高速收费系统的规模，本路段态势感知平台分析能力为 1.5G。

4.2. 态势感知数据分析平台

根据省中心文件要求，路段级态势感知数据分析平台主要包括网络安全分析、资产管理与分析、溯源取证功能、安全态势呈现、威胁情报、安全运营等功能。

4.2.1 网络安全分析能力

（1）大数据分析能力

态势感知大数据分析平台基于大数据分析架构，对所有数据进行分析，主要包括：KAFKA 消息队列、Apache Storm 实时流式计算引擎、HBASE 数据存储技术、Apache SPARK 迅捷数据分析引擎、Deep Learning 深度学习技术、ElasticSearch 高速数据存储/查询技术。

基于大数据分析平台数据分析层的处理能力，针对性地对路段中心关注度级别较高的安全事件进行独立模块化模块化分析展示，如高危攻击、恶意文件、C&C 攻击、邮件威胁、网页篡改、暴力破解、拒绝服务、异常访问、高危漏洞等。

（2）威胁分析能力

威胁分析子系统通过从内部威胁、外连威胁、外部威胁、文件威胁等多个层面对网络安全威胁进行细化分析呈现。针对单个失陷资产，可完整关联该失陷资产的威胁扩散范围，针对单个恶意文件，可精准关联该文件在网络中的传播范围，并图形化展示，帮助用户快速定位失陷范围，进而提升问题排查处置效率。

（3）流量分析能力

基于资产维度的流量访问关系，分别对内部流量、外部流量、外连流量进行呈现和分析。可直观呈现资产之间访问关系以及访问协议类型，结合安全事件分析子系统，可关联到攻击手段、攻击次数等信息，为事后溯源取证提供参考依据。

应用深度学习技术建立流量模型，进一步提升违规网络行为检测的准确率和检出率。

同时支持用户自定义流量模型，满足不同行业的用户在不同场景检测违规网络行为的需求。

4.2.2 资产管理与分析能力

可识别服务器（业务服务器、数据库服务器、WEB 服务器、远程管理服务器、代理服务器等）、终端（手机、摄像头、打印机、媒体设备等）、网络设备（交换机、防火墙、无线设备等），通过 Iprobe 引擎结合多种流量协议：SSH、Telnet、Onvif 等，对目标资产进行多维度信息探测，结合资产库、CMS 指纹库进行综合数据分析处理，最终在业务上形成可视化呈现。以资产维度呈现整网风险态势，支持对资产所属机构、责任人、资产标签等自定义添加，从纵向、横向两个维度简化资产管理运维难度。

4.2.3 溯源取证能力

（1）流量存储与统计分析

采用分布式存储技术，通过对关键业务流量进行全包解析存储及元数据提取，实现流量分析、数据钻取、威胁溯源及审计取证等功能，支持自定义解析存储策略，存储与违规行为相关的解析流量。回查历史网络流量的原始数据，提供网络流量的原始数据包存储和回溯查询能力，可对链路流量、应用流量、故障告警相关流量、指定主机流量进行精准的追溯分析。从多角度还原历史场景，重组完整的会话信息。多维度展示网络中的流量组成和网络行为。提供端到端的全流量行为、性能的可视化分析能力，提升用户对网络与应用的可视化管理能力，为网络调整提供可信的决策依据。

（2）黑客画像

针对攻击者的行为特点、常用工具、攻击请求的指纹。黑客画像系统预置了对应的黑客攻击知识库，通过从流量上提取特征，可以有效的发现攻击者使用的工具。我们通过攻击者发送的攻击请求的一些行为特点和流量特点，可以提取攻击者发起攻击的浏览器、操作系统版本信息，通过历史数据的积累和分析，可以进一步的分析出攻击者使用仿冒浏览器攻击的可能性。

（3）基于 ATT&CK 模型的分析

基于 ATT&CK 框架的攻击矩阵分析：内置攻击矩阵知识库，支持将安全事件划分至 13 个入侵阶段，入侵阶段包括但不限于：扫描探测、投放利用、代码执行、持续突防、权限提升、防御绕过、账户破解、环境洞察、横向扩散、数据采集、命令控制、数据窃取、造成影响；对单次安全事件中涉及的入侵阶段以及使用的攻击技术有明显标注，支持针对使用的每个攻击技术进行具体分析展示。

4.2.4 安全态势呈现

安全态势呈现主要从资产、脆弱性、病毒态势、威胁以及综合态势五个维度对整网安全进行实时监控。

资产监控：可呈现资产盘点统计情况、资产告警及风险统计情况以及最新资产动态等内容；

脆弱性监控：可呈现整网资产漏洞情况（包括漏洞分布、类型、级别等）、脆弱性资产统计，可动态展示最新发现的漏洞情况；

病毒监控：可展示感染恶意文件资产类型及数量、恶意文件传播总数及高危文件类型传播次数、恶意文件类型 Top、恶意文件家族 Top、恶意文件源 Top 等统计信息。

威胁监控：可呈现外部威胁、外联威胁、内部威胁等维度的安全事件告警统计情况以及高危事件 Top、攻击趋势、攻击类型等内容，同时可动态展示实时发现的安全事件情况；

综合态势监控：结合资产、脆弱性、威胁等多方面数据，可动态地呈现资产 IP 的安全风险趋势、整网漏洞风险情况、不同级别攻击的威胁走势等。

基于以上细粒度的监控内容，结合直观的可视化呈现，可帮助用户快速识别网络异常入侵行为，掌握整网资产状态、漏洞状态，及时把握网络安全事件发展趋势，为用户营造全新安全管理体验。

4.2.5 威胁情报能力

威胁情报系统的数据来源包括了探针扫描检测数据、日志分析数据、专业安全服务单位定期更新情报以及第三方威胁情报；用户可以提交可以的文件、域名、URL、IP 等进行一键查询，威胁情报关联子系统将返回检测结果及报告；威胁情报系统基于大数据技术可进行机器学习与大数据关联分析，大大提高了威胁情报的准确性。

4.2.6 安全运营能力

支持与省级态势感知平台对接，实现节点注册接口、节点状态同步接口、工单接口、事件上传接口、事件处理结果上传接口、安全告警数据上传接口、安全扫描数据上传接口、资产信息主动上传接口、情报共享接口的对接。

4.3.安全探针

安全探针用于采集区域/路段中心域系统的网络安全信息，并进行一定的分析和提取，向态势感知数据分析平台提供数据和分析结果。

根据安全探针的不同采集功能，分为以下两种类型：

1）态势感知全流量检测探针

态势感知全流量检测探针主要采集的区域/路段中心域系统流量分析数据，采集对象应包括但不限于：漏洞利用检测分析数据、webshell 攻击检测分析数据、木马与间谍软件检测分析数据、恶意文件检测分析数据、异常报文流量检测分析数据、C&C 通信检测分析数据、恶意邮件检测分析数据等。

2）态势感知脆弱性检测探针

态势感知脆弱性检测探针主要采集资产数据和安全扫描数据。

采集的区域/路段中心域系统的资产数据，采集对象应包括但不限于：资产名称、资产 IP 地址、资产的类型数据、资产操作系统数据、资产厂商信息数据、资产所属业务系统数据、资产开放服务数据等。

采集的区域/路段中心域系统的安全扫描数据，采集对象应包括但不限于系统漏洞情况、 Web 应用漏洞情况、高危端口情况、弱口令情况。

4.4.运维期服务要求

本路段态势感知平台建成后系统的年运营经费包括运营托管服务、驻场护网服务和回溯分析和报表服务等三项内容：

1) **运营托管服务。**本项服务为托管服务，服务单位应提供以下内容（包括但不限于）：基于本地数据和云端威胁情报分析、态势感知平台告警进阶分析验证、现网安全网络安全运行状态阶段性总结、高危风险项整改指导建议、高危风险项整改复测等方面。并通过态势感知监测数据实时同步业主相关报告并指导业主整改。
2) **驻场护网服务。**根据业主要求进行驻场服务，针对部省安排的收费系统护网行动、攻防演练等提供专业人员驻场值守服务，协助路段运营单位完成专项行动并提供及时的技术指导。

3) **回溯分析和报表服务。**每年不少于 4 次（每季度 1 次）对本路段态势感知平台发现的实践进行回溯分析和判断并形成报告，并根据报告内容提出专业性意见和建议，指导本路段运营单位进行相关整改工作。

4.5.其他要求

本次建设所采用的平台应满足省中心文件中相关要求，安全探针部署在路段收费系统核心交换机处，由于台州高速收费系统现有核心交换机已没有剩余端口，因此本次设计新增 1 台交换机接入现有交换机作为镜像，安全探针接入镜像交换机获取流量和数据。

安全探针应支持收费系统网内各类资产的信息采集并对接其他安全类设备，获取其开放的告警信息、预警信息和相关事件处理信息等安全信息。

根据省中心文件要求路段态势感知平台需要与省平台对接，相关接口参见《浙江省高速公路联网收费系统网络安全态势感知平台体系建设方案》中《附件：浙江省收费公路联网收费系统网络安全态势感知平台体系接口对接标准》。

4.6.主要工程数量

台州高速路段态势感知平台建设主要工程量如下：

序号	设备名称	规格、说明	单位	数量
1	态势感知数据分析平台	1.5G 分析能力	套	1
2	态势感知全流量检测探针	单台≥1.5Gbps 流量采集能力	套	1
3	态势感知脆弱性检测探针	512 个地址扫描授权	套	1
4	镜像交换机	交换容量≥384Gbps	套	1

4.7 主要设备技术指标

根据本路段收费系统的规模，按照 1.5G 流量确定相关设备性能指标。

4.7.1 态势感知数据分析平台

- CPU≥16 核，万兆光口≥2，千兆电口≥2，内存≥64G，冗余电源，单电源功率≥550W，硬盘≥8T；单台≥1.5Gbps 流量处理性能

- 具备大数据架构，采用 Hbase、Kafka、Storm、Spark、ElasticSearch 大数据功能组件，平台可监控各组件运行状况；
- 具备网络安全分析功能，支持单一资产原始流量分析，支持在访问关系维度查看不同访问方式、不同访问方向的流量统计列表以及访问关系图；
- 具备资产监控及分析功能，通过流量被动识别、主动探测、手动录入等不少于三种方式生成现网资产列表
- 具备高危漏洞的专项检测能力，并针对高危漏洞平台自动化进行验证、判断；
- 具备溯源取证功能，基于国际先进的攻击链模型和时间轴进行溯源分析；
- 具备安全态势呈现功能，基于攻击者 IP、受害者 IP、攻击源端口、攻击目的端口、攻击类型、攻击名称等属性作为过滤条件进行网络攻击自定义监控；
- 具备独立的威胁情报检索功能；
- 具备安全运营功能，支持与省级态势感知平台进行联动，实现所有功能接口的对接，将相关安全信息上传至省级态势感知平台，并接收省级态势感知平台下发的指令。
- 3 年硬件质保和 3 年平台软件升级

4.7.2 态势感知全流量检测探针

- CPU≥16 核，万兆光口≥2，千兆电口≥2，内存≥64G，冗余电源，单电源功率≥550W，硬盘≥1T；单台≥1.5Gbps 流量采集能力；
- 具备标准模式、增强模式、深度模式、专家模式等不少于四种流量分析策略；
- 具备全流量检测引擎,可实现 IP 碎片重组、TCP 流重组、应用层协议识别与解析，能够对网络通信行为进行识别；
- 具备检测命令注入、目录遍历、口令暴力破解、信息泄露探测、Webshell 上传、代码注入等 Web 漏洞攻击能力；
- 具备目录遍历、跨栈脚本攻击、文件上传、命令注入、SQL 注入、配置文件错误等主机漏洞攻击的正反向检测能力；
- 具备应用程序漏洞攻击、数据库漏洞攻击、DNS 漏洞攻击、文件漏洞攻击、FTP 漏洞攻击等系统及应用层攻击检测的能力。
- 3 年硬件质保

4.7.3 态势感知脆弱性检测探针

- 双电源，CPU≥4 核，内存≥16GB，存储≥1T，USB 接口≥2 个，千兆电口≥8 个，接口扩展槽≥1 个，支持扩展 4 千兆电口和 4 千兆光口；最大并发任务数 5 个，**实配 256 个地址扫描授权；**
- 具备丰富资产指纹库及自主研发的识别引擎，可基于 A 段、B 段创建下发资产盘点任务对目标资产进行多维度信息探测；
- 具具备高危漏洞的专项检测能力，适用于服务器、业务系统等设备极多的网络环境下快速安全检测；
- 具备漏洞自动化验证功能，自动化验证功能不需要任何人进行参与，平台自动对漏洞进行验证、判断，最后生成包含漏洞验证成果（漏洞截图）的检测报告；
- 具备边界完整性检查功能，可检测出目标设备连接智能手机热点、通过智能手机 USB 共享网络等违规双网卡共享外联行为，可检测出私接 WI-FI、BYOD 设备。
- 3 年硬件质保

4.7.4 交换机

- 产品类型：万兆以太网交换机
- 应用层级：三层
- 传输速率 10/100/1000Mbps/10Gbps
- 交换方式：存储-转发
- 交换容量：2.5Tbps 以上
- 端口数量：26 个
- 端口描述：24 个 10/100/1000M 以太网口，2 个 1/10G SFP+扩展槽（光模块暂不配置）

功能特性：

- 支持静态路由、RIP、OSPFv3，GBP,ISIS
- 支持等价路由，路由策略，VRRP，策略路由
- 支持 DHCP
- 支持 Tunnel

- 支持组播
- 支持链路聚合
- 支持流量控制
- 支持 RRPP
- 支持端口镜像
- 支持 VLAN

其它参数

- 电源电压 AC 115-240V，50-60Hz，12-6A
- 平均无故障时间≥100000 小时

环境标准

- 相对湿度：10%-90%，无冷凝
- 工作环境温度：0-45℃