ARGUS系统

《概要设计说明书》

2018年9月7日

北京航空航天大学计算机学院

**修订版本**

|  |  |  |  |
| --- | --- | --- | --- |
| **版本** | **修订人** | **日期** | **备注** |
| V1.0 | 夏涛 | 2018.9.5 | 初稿 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**目录**

[1 引言 5](#_Toc524082098)

[1.1 编写目的 5](#_Toc524082099)

[1.2 读者对象 5](#_Toc524082100)

[1.3 项目背景 5](#_Toc524082101)

[1.4 参考文献 6](#_Toc524082102)

[2 任务概述 7](#_Toc524082103)

[2.1 目标 7](#_Toc524082104)

[2.2 用户特点 7](#_Toc524082105)

[2.3 假设和依赖 7](#_Toc524082106)

[3 具体需求 8](#_Toc524082107)

[3.1 功能需求 8](#_Toc524082108)

[3.1.1 系统首页 8](#_Toc524082109)

[3.1.2 检索结果页面 8](#_Toc524082110)

[3.1.3 设备地图 9](#_Toc524082111)

[3.1.4 漏洞库 9](#_Toc524082112)

[3.1.5 态势感知 10](#_Toc524082113)

[3.1.6 城市工控设备状况 10](#_Toc524082114)

[3.2 外部接口需求 11](#_Toc524082115)

[3.2.1 用户接口 11](#_Toc524082116)

[3.2.2 硬件接口 11](#_Toc524082117)

[3.2.3 软件接口 11](#_Toc524082118)

[3.2.4 通信接口 11](#_Toc524082119)

[3.3 性能需求？ 11](#_Toc524082120)

# 引言

## 编写目的

此文档是对ARGUS系统功能、性能、用户界面以及运行环境，系统部署条件等信息做出详细说明。为系统设计阶段提供依据和指导。帮助开发人员、测试人员和相关人员了解系统实现的功能，并作为验证产品是否能满足用户需求的依据。

## 读者对象

此文档面向的读者人群为：参与此项目的前端开发人员、后端开发人员、测试人员、项目经理以及市场营销人员。

## 项目背景

随着信息化的快速发展和工业化水平的不断提升，互联网发展与新工业革命的历史性交汇催生了工业互联网，工业变革今后的发展趋势将是数字化、网络化、智能化。安全问题日益成为工业互联网发展过程中不容忽视的关键因素。

在中国提出《中国制造2025行动纲要》后，工业互联网已经是国家战略组成，工业互联网安全关系国家战略安全。工业互联网中工业网络与采用Internet 技术的商业网络的打通，标准Internet 的威胁也随之而来—— 病毒和黑客。原本认为不容易被攻击的工业网络，也因存在设备同时连接到企业网络，而使该设备成为攻击跳板，最后工业网络受到攻击。给企业造成。工业互联网主要受到来自六个层次的威胁：设备安全、网络安全、控制安全、数据安全、应用安全和参与全程的人员安全。

为了应对日益严峻安全的挑战，企业和组织采取了相应的应对措施：对自身的工业设备进行登记、采用蜜罐技术对入侵行为进行捕获分析、网络分区防护等等，一定程度上起到了维护自身工业设备安全作用。

态势感知是指综合分析工业互联网安全要素，结合企业、商业网络和工业网络状态，评估工业互联网的安全状况，预测其变化趋势，以可视化的方式展现给用户，并给出相应的应对措施和报表。在中国，将态势感知技术用于互联网、企业内网已经出现了解决方案，如360 公司的天眼下一代态势感知和未知威胁发现平台，但是将态势感知用于工业互联网在国内还是比较少的。然而，随着工业互联网建设的不断推进，政府和组织对于工业互联网设备的安全态势有更清晰了解的需求与日俱增。

## 参考文献

[1]刘多. 全面加强工业互联网安全能力建设. <https://wenku.baidu.com/view/29f5e0b9a48da0116c175f0e7cd184254a351b6c.html>

[2] 陶耀东，李强，李宁，工业互联网的安全挑战及应对策略 [J]. 中兴通讯技术,2016,22(5):36-46

# 任务概述

## 目标

ARGUS系统是一款支持按不同字段（ip、country、city、protocol等）对工业联网设备进行搜索、漏洞收集和统计、安全态势感知、城市工控设备安全状况统计等功能的工业安全状况分析系统（系统定位）。

根据项目的计划，项目的目标主要是实现以下几个方面的功能：

1. 工业联网设备搜索；
2. 设备漏洞的收集和统计
3. 安全态势感知
4. 城市工控设备安全状况统计分析（国内？）

## 用户特点

主要用户是各个企业、工厂的安全管理人员、系统运维人员、政府工业安全部门的负责人、监管人员等。用户需要对系统运维、linux操作系统、windows操作系统、Internet协议、工业互联网、网络安全以及各种类型的工业设备有一定的了解。

## 假设和依赖

本项目能否成功实施取决于以下条件:

1. 研发团队掌握了先进的能适用于该项目的技术，这是系统的性能是否优化、项目能否完成的根本保证；
2. 团队成员的积极配合，为了项目的开发和实施，合理规划个人时间同时为团队做出合理牺牲，配合队友完成任务。

# 具体需求

## 功能需求

### 系统首页

**图1首页原型图**

功能描述：

1. 工业联网设备搜索框，用户通过按输入规则输入相应字段可以得到查询结果，当光标位于输入框时提示用户检索的输入规则；
2. 系统支持的工业协议（和可以扫描到的端口？），用户可以点击相应的协议和端口快速查看搜索结果。
3. 页面右上方显示系统所有的展示页面按钮，用户点击相应的按钮进入相应的展示页面。

### 检索结果页面

**图2搜索结果页面原型图**

功能描述：

此页面主要用于展示用户搜索的结果。主要展示设备的基本信息：满足用户输入搜索条件的全部设备总数，所耗时间，设备IP，国家（以国旗方式显示），城市，设备收录时间，设备所在位置经纬度信息，端口号，设备使用协议，设备名称。对于能够收集到详细信息的设备要向用户展示详细的信息。

### 设备地图

**图3设备地图原型图**

功能描述：

此页面主要通过卫星地图展示系统所能探测到的工业设备，地图要能够放大和缩小，使用带有不同颜色的亮点标识各个设备，并随着地图的不断放大逐级展示所探测到的设备。点击设备亮点能够显示设备的基本信息（IP,端口,国家,城市,设备类型,探测到的时间），页面右侧可以通过筛选不同的设备协议来在地图上显示所探测到的设备。要能够把摄像头和其他工业设备区分开。

### 漏洞库

**图4漏洞搜索展示页面原型图**

功能描述：

用于为用户提供检索系统中所收录的漏洞，本系统主要收录CVE和CVND中的漏洞信息。进入漏洞搜索页面应能够要为用户提供漏洞搜索框，搜索结果要展示漏洞的名称，危害等级，发布时间等基本信息，点击相应的漏洞要能够展示漏洞的详细信息。此外要提供按年份和漏洞数量所绘制的曲线统计图和统计不同危害等级漏洞数量的饼状图。

### 态势感知

**图5态势感知页面原型图**

功能描述：

态势感知主要用于展示系统所能探测到的攻击行为并做一些简单的统计。此页面应能显示出系统所探测到的所有攻击的次数，列出前几个攻击源的位置和攻击次数，前几个攻击目标的位置和受攻击的次数，以及前几个攻击类型和攻击次数。以表格形式展示统计的结果。要能够动态实时的显示攻击行为。包括攻击的时间，攻击者，攻击IP，攻击位置，目标位置，攻击类型和端口。攻击端口要能够可选。用户可以选择不同的端口获取相应的攻击的信息。此外要能够通过攻击动画更形象的展示攻击过程。

### 城市工控设备状况

**图6城市工控设备状况原型图**

功能描述：

针对某一城市对城市的工控设备安全状况进行详细的分析，将统计分析结果展示给用户。具体包括：1.系统所能探测到的城市联网工控设备总量 2.设备协议占比饼状图 3.历史变化趋势图 4.城市地图，按 5.工控品牌分布图 6.最新扫描到的漏洞 7.各区的工控设备占比图。

## 外部接口需求

### 用户接口

用户界面的相关需求已在功能需求部分描述

### 硬件接口

无特殊需求

### 软件接口

无特殊需求

### 通信接口

无特殊需求

## 性能需求？

尚未形成完整文档