ARGUS系统

《需求说明书》

2018年9月5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](#_Toc24087)

[1.1 编写目的 5](#_Toc26521)

[1.2 读者对象 5](#_Toc12404)

[1.3 项目背景 5](#_Toc6322)

[1.4 参考文献 6](#_Toc32441)

[2 任务概述 7](#_Toc31444)

[2.1 目标 7](#_Toc7329)

[2.2 用户特点 7](#_Toc21197)

[2.3 假设和依赖 7](#_Toc958)

[3 功能性需求 8](#_Toc17404)

[3.1系统首页 8](#_Toc25020)

[3.1.1：用户自定义搜索功能 8](#_Toc9729)

[3.1.2：支持按设备协议和端口进行快速搜索功能 8](#_Toc5592)

[3.1.3：导航功能 8](#_Toc4307)

[3.2设备地图 8](#_Toc32529)

[3.2.1：在卫星地图上展示搜索到的全部设备功能 9](#_Toc6837)

[3.2.2：按协议筛选设备功能 9](#_Toc18653)

[3.3检索结果页面 9](#_Toc24224)

[3.3.1：用户自定义检索功能 10](#_Toc4697)

[3.3.2：显示搜索到的设备数量和所耗时间 10](#_Toc22291)

[3.3.3：展示设备基本信息功能 10](#_Toc27745)

[3.3.4：分页展示功能 10](#_Toc14454)

[3.4漏洞库 10](#_Toc19690)

[3.4.1：漏洞检索功能 10](#_Toc3945)

[3.4.2：漏洞搜索结果展示功能 11](#_Toc19082)

[3.4.3：支持近17年的漏洞发布数量折线统计图 11](#_Toc19128)

[3.4.4：支持漏洞危害等级扇形统计图 11](#_Toc18730)

[3.4.5:漏洞统计 11](#_Toc21967)

[3.5态势感知 13](#_Toc18720)

[3.5.1显示当前攻击总量功能 13](#_Toc20445)

[3.5.2：静态展示功能 13](#_Toc21577)

[3.5.3：动态展示攻击信息功能 13](#_Toc3339)

[3.5.4：攻击动画功能 14](#_Toc8420)

[3.6城市工控设备状况信息展示功能 14](#_Toc14961)

[3.6.1：上海市工控设备数量 14](#_Toc48)

[3.6.2:上海市设备协议占比 14](#_Toc689)

[3.6.3：城市地图展示功能 14](#_Toc7971)

[3.6.4：工控品牌分布柱状图 14](#_Toc16476)

[3.6.5：最新扫描结果滚动显示功能 15](#_Toc4532)

[3.6.6：城市各区工控数量占比扇形统计图 15](#_Toc29839)

[3.6.7：近七天城市设备数量变化趋势曲线图 15](#_Toc9610)

[4.非功能性需求 15](#_Toc11111)

[4.1外部接口需求 15](#_Toc7952)

[4.1.1用户接口 15](#_Toc1351)

[4.1.2硬件接口 15](#_Toc23612)

[4.1.3软件接口 15](#_Toc4860)

[4.1.4通信接口 16](#_Toc29330)

[4.2性能需求 16](#_Toc25662)

# 引言

## 编写目的

此文档是对ARGUS系统的功能、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。

# 功能性需求

## 3.1系统首页

**图1首页原型图**

### 3.1.1：用户自定义搜索功能

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设备的输入规则。

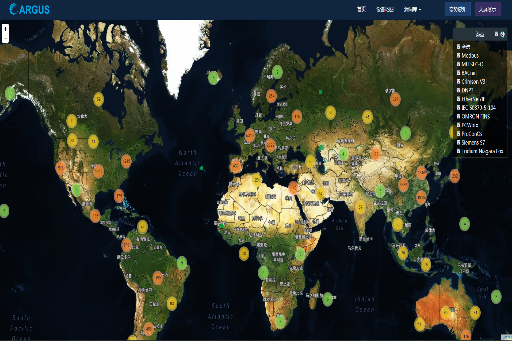
### 3.1.2：支持按设备协议和端口进行快速搜索功能

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。支持快速检索的协议有：HTTP，Modbus，Siemens s7，IEC 60870-5-104，DNP3，EtherNet/IP，BACnet，Tridium Niagara Fox，Crimson V3，PCWorx，ProConOs，MELSEC-Q，ATG。端口有：80,502,102,2404,20000,44818,47808,1911,789,9600,1962,20547,5007,10001。

### 3.1.3：导航功能

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。

## 3.2设备地图

**图3设备地图原型图**

### 3.2.1：在卫星地图上展示搜索到的全部设备功能

在卫星地图上显示系统所能搜索到的设备，每一个设备都以带颜色的亮点显示在地图上，点击亮点能够显示该设备的基本信息：IP，Port，country，city，type，timestamp。设备地图要能够放大和缩小，所有设备不是一下子全部展示在地图上，随着地图不断放大设备逐级显示在地图上。

### 3.2.2：按协议筛选设备功能

页面右侧有系统所支持的协议的勾选框：Modbus，Siemens s7，IEC 60870-5-104，DNP3，EtherNet/IP，BACnet，Tridium Niagara Fox，Crimson V3，PCWorx，ProConOs，MELSEC-Q，用户可以通过勾选不同的设备协议来在地图上显示所探测到的设备。摄像头勾选框用来区分摄像头和其他工业设备，用户可以选择是否在设备地图上显示摄像头设备。

## 3.3检索结果页面

**图2搜索结果页面原型图**

### 3.3.1：用户自定义检索功能

工业联网设备搜索框，功能同首页的设备搜索框。

### 3.3.2：显示搜索到的设备数量和所耗时间

显示满足用户输入的搜索条件的所有设备数量，和所耗时间。

### 3.3.3：展示设备基本信息功能

向用户展示所搜索到的每一个设备的基本信息主要包括：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，设备名称设备的详细信息展示在相应设备的后方。

### 3.3.4：分页展示功能

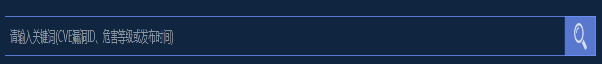
每页展示10个搜索到的设备，采用分页的方式逐页展示搜索到的全部结果。

## 3.4漏洞库

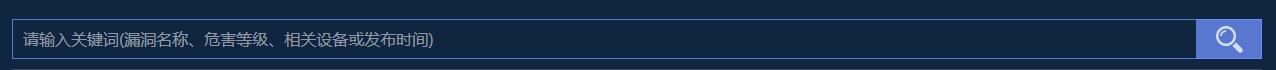
**图4漏洞搜索展示页面原型图**

### 3.4.1：漏洞检索功能

漏洞检索框，用户通过输入漏洞ID，漏洞名称，相关设备，危害等级，发布时间等在漏洞库中对漏洞进行检索。

CVE漏洞库中搜索框中提示：

CVND漏洞库搜索框提示：



### 3.4.2：漏洞搜索结果展示功能

展示用户搜索的漏洞结果的基本信息，以列表方式展示：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| CVE漏洞库 | 漏洞ID | 危害等级 | 发布时间 |  |
| CVND漏洞库 | 漏洞名称 | 危害等级 | 相关设备 | 发布时间 |

采用分页的方式展示搜索漏洞结果，每页展示11个结果，逐页展示。

### 3.4.3：支持近17年的漏洞发布数量折线统计图

绘制标题为漏洞发布时间的折线统计图，统计图以年份为横坐标（2002-2016）对应年份发布的漏洞数量为纵坐标。主要用于展示从2002-2016年每年漏洞发布数量的变化情况。鼠标选中折线图上的点时，可以显示对应的年份和和该年份发布的高危工控漏洞的数量。

### 3.4.4：支持漏洞危害等级扇形统计图

绘制标题为漏洞危害等级的扇形统计图，该图按高中低三个等级以不同的颜色表示三个危害等级的漏洞的数量占全部漏洞数量的比例，鼠标选中每一块扇形区域时，该区域要能够突出显示，并能显示该区域表示的危害等级，漏洞数量，占漏洞总数的比例。

### 3.4.5:漏洞统计

漏洞统计部分主要包含4个统计图。

#### (1).国家设备厂商的分布扇形统计图

此图包含的国家为：中国台湾，日本，以色列，法国，印度，马来西亚，英国，丹麦，中国，瑞士，意大利，奥地利，阿根廷，加拿大，德国，瑞典。扇形统计图主要表示以上国家各自的厂商数量及所占全部厂商数量的比例。鼠标拖到相应的扇形区域时，该区域能够突出显示，并能以文字方式显示国家名称，厂商数量和所占比例。在页面左端有选择按钮，可以通过点击相应国家的按钮来决定该国家是否在统计图中显示。

#### (2).设备的漏洞分布扇形统计图

此图主要展示不同设备的漏洞数量和所占比例。此图中展示的设备为：控制器，SCADA/HMI，管理工具，PLC，HMI，others，DCS，SCADA当鼠标拖到不同的扇形区域时，扇形区域要能够突出显示，并能显示该扇形区域所表示的设备类型，漏洞数量和所占比例。在页面左端有选择按钮，可以通过点击相应类型设备的按钮来决定是否在统计图中显示该类型的设备。

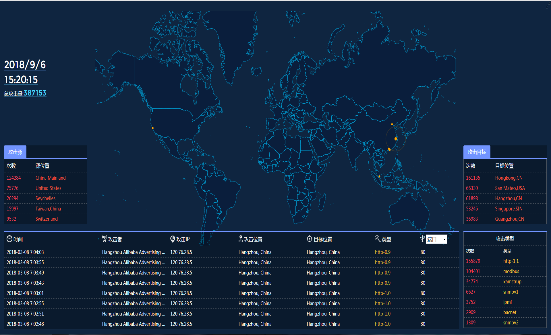
#### (3).厂商的漏洞数量柱状统计图

此图主要展示漏洞数量排名前十的厂商的漏洞数量，当鼠标拖到某一柱状区域时，要能够以文字方式显示该条柱状表示的厂商的名称和漏洞设备量

#### (4).13种主流协议的漏洞数量柱状统计图

此图中显示的是主流的13种协议的漏洞的数量。协议包括： Modbus，Siemens s7，IEC 60870-5-104，DNP3，EtherNet/IP，BACnet，Tridium Niagara Fox，Crimson V3，PCWorx，ProConOs，MELSEC-Q，ATG。当鼠标拖到某一柱状区域时能够以文字方式显示该柱状区域表示的协议名称和漏洞数量。

## 3.5态势感知

**图5态势感知页面原型图**

### 3.5.1显示当前攻击总量功能

要能够实时显示日期和时间以及总攻击的总量。

### 3.5.2：静态展示功能

要在态势感知页面中显示三个表格，攻击源，攻击目标，攻击类型。

攻击源表格：5行2列显示按攻击次数从高到低的顺序排序的前五个攻击源的位置和攻击次数。

攻击目标列表：5行2列显示按受攻击次数从高到低的顺序排序的前五个被攻击目标的位置和受攻击的次数。

攻击类型列表：7行2列显示按攻击次数从高到低顺序排序的前七个攻击类型和攻击次数。

### 3.5.3：动态展示攻击信息功能

态势感知页面要能以列表的方式滚动显示攻击的基本信息：攻击时间，攻击者，攻击IP，攻击位置，目标位置，攻击类型和端口，端口可以由用户自行选择，用户选择不同的端口时，能够显示相应端口的攻击信息。

### 3.5.4：攻击动画功能

攻击动画，模拟攻击行为。在地图上标注出蜜罐的位置，用动画方式演示攻击行为。

## 3.6城市工控设备状况信息展示功能

**图6城市工控设备状况原型图**

### 3.6.1：上海市工控设备数量

在城市设备地图上要能够显示上海市全部的工控设备数量。

### 3.6.2:上海市设备协议占比

设备协议占比扇形统计图。显示主流的13种协议的工控设备数量在上海市的分布情况，主流的13种协议同漏洞统计页面中所提到的协议。当鼠标移动到相应的扇形区域时，该扇形区域要能够突出显示，并能以文字方式显示该区域所表示协议的名称和设备数量和该协议设备数量占上海市全部设备的比例。

### 3.6.3：城市地图展示功能

要能够显示上海市的全部地图，并能按区显示各区的工控设备的数量。以颜色变化体现设备数量的多少，鼠标拖动到各区的地图上时，以文字显示该区的设备数量，当选中该区时该区的地体图变为蓝色。

### 3.6.4：工控品牌分布柱状图

主要统计上海市的RocwellAutomation和Siemens的设备数量。当鼠标拖动到相应的柱状区域时以文字方式显示该区域的工控品牌名称和相应的设备数量。

### 3.6.5：最新扫描结果滚动显示功能

以滚动方式显示最新扫描到的漏洞信息

### 3.6.6：城市各区工控数量占比扇形统计图

统计上海市各区的工控设备数量，以不同的颜色表示上海市的各个区，当鼠标拖动到某个扇形区域时，该区域要能够突出显示，并以文字方式标注出该区的名称和设备数量占全市设备总数的比例。

### 3.6.7：近七天城市设备数量变化趋势曲线图

该图主要展示2018.8.14-2018.9.4上海市设备的变化趋势情况，选取了这段时间内的几天时间（08.14,08.15,08.18,08.23,08.28,08.29,08.30,09.02，09.03，09.04）的设备变化趋势情况，绘制了曲线图。当鼠标拖动到图上的点时能够以文字方式显示日期和该天的变化趋势。

# 4.非功能性需求

## 4.1外部接口需求

### 4.1.1用户接口

用户界面的相关需求已在功能需求部分描述

### 4.1.2硬件接口

无特殊需求

### 4.1.3软件接口

无特殊需求

### 4.1.4通信接口

无特殊需求

## 4.2性能需求

尚未形成完整文档