第 36 卷　第 5 期　　计　算　机　工　程　　2010 年 3 月
Vol.36　No.5　　Computer Engineering　　March 2010
·工程应用技术与实现·　文章编号：1000—3428(2010)05—0228—03　文献标识码：A　中图分类号：TP319

# EPA 网络安全组态技术

王　平，陈　洲，刘思东，王　珽
(重庆邮电大学网络化控制与智能仪表教育部重点实验室，重庆 400065)

**摘　要：**针对工业控制中 EPA 网络的网关安全问题，基于 EPA 组态软件，提出 EPA 网络安全组态技术。设计 EPA 网络安全组态模块，通过组态功能块定义访问控制对象，设置加密密钥、校验密钥、校验算法。访问控制对象经编译后下载到安全设备中，决定安全设备的运行状态。测试结果表明，该技术可提升工业控制领域 EPA 网络控制的安全性和可靠性。

**关键词：**EPA 协议；功能块；安全组态；设备鉴别；访问控制对象

# EPA Network Security Configuration Technology

**WANG Ping, CHEN Zhou, LIU Si-dong, WANG Ting**
(Key Laboratory of Network Control & Intelligent Instrument, Ministry of Education,
Chongqing University of Posts and Telecommunications, Chongqing 400065)

**【Abstract】**Aiming at Ethernet for Plant Automation(EPA) network gateway security control problem of industrial control, this paper proposes EPA network security configuration technology based on EPA configuration software. It designs EPA network security configuration module, realizes access control object through configuration of function block, set encrypt key, checkout key and checkout arithmetic. Access control object is download to safe device after translation and edition to decide the run state of safe device. Test result shows that this technology can effectively satisfy the design of EPA control system and the needs of security, and enhance the safety and reliability for EPA network control in the field of industrial control network.

**【Key words】**Ethernet for Plant Automation(EPA) protocol; function block; security configuration; device authentication; access control object

EPA(Ethernet For Plant Automation)标准面向控制工程师的应用，利用基于 EPA 通信规范与 EPA 网络安全规范[1-2]，IEC61499 标准和 IEC61804 标准定义开放、分布式、可重用的自控系统基本模块(如功能块)，通过易实现的连接关系联系，组成分布式现场网络控制系统，以满足不同工程应用的要求。随着 EPA 的发展，其工控网络安全性已成首要问题。本文基于《用于工业测量与控制系统的 EPA 系统结构与通信标准》提出并实现了 EPA 工业控制网络安全组态技术。

## 1　EPA安全网络结构

EPA 安全网络结构如图 1 所示。

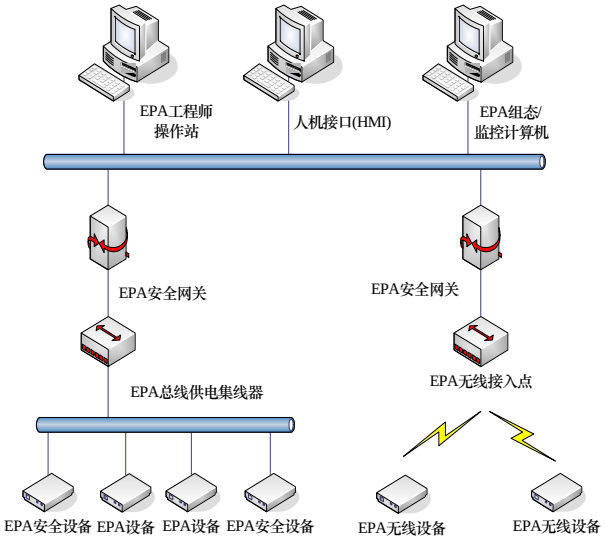


**图 1　EPA 安全网络结构**

在 EPA 安全网络中，EPA 安全网关不仅起到分隔 EPA 微网段的作用，同时为现场设备层网络提供边界保护。EPA 安全网关包含完整实现的 EPA 安全协议栈，位于应用层的 EPA 安全实体，以及位于网络层和数据链路层的 EPA 报文控制管理实体。EPA 报文控制管理实体提供防火墙和地址转化功能，对出入 EPA 微网段的所有数据包进行控制，保护 EPA 设备免于各种非 EPA 报文的攻击。EPA 网络安全管理实体通过 EPA 安全措施，保护微网段内设备免于 EPA 报文的攻击。

## 2　EPA网络安全组态的总体架构

### 2.1　子模块的划分

EPA 网络安全组态[3-5]是 EPA 组态软件中很重要的模块，其作用是防止非法设备接入 EPA 网络，防止 EPA 网络数据被非法篡改，保护 EPA 网络数据被非法获取，设置 EPA 安全设备之间的访问权限。根据以上要求将 EPA 网络安全组态划分为 4 个子模块：设备鉴别处理，访问控制管理，数据报文加密管理，数据报文校验管理。

### 2.2　子模块之间的结构关系

EPA 设备鉴别处理子模块是整个 EPA 网络安全组态的基础，该子模块用于鉴别 EPA 网络中设备的合法性。只有通过 EPA 设备鉴别处理的设备组态软件才能对该设备设置访问权

**基金项目：**国家“863”计划基金资助重点项目“基于 EPA 的应用系统开发”(2007AA041301)
**作者简介：**王　平(1963－)，男，教授、博士、博士生导师，主研方向：工业以太网及网络控制，无线传感器网络，工业无线通信；陈　洲、刘思东，硕士研究生；王　珽，副教授
**收稿日期：**2009-08-11　**E-mail：**cz821121@163.com

限，选择报文加密算法，选择数据校验算法。EPA 网络安全组态结构如图 2 所示。

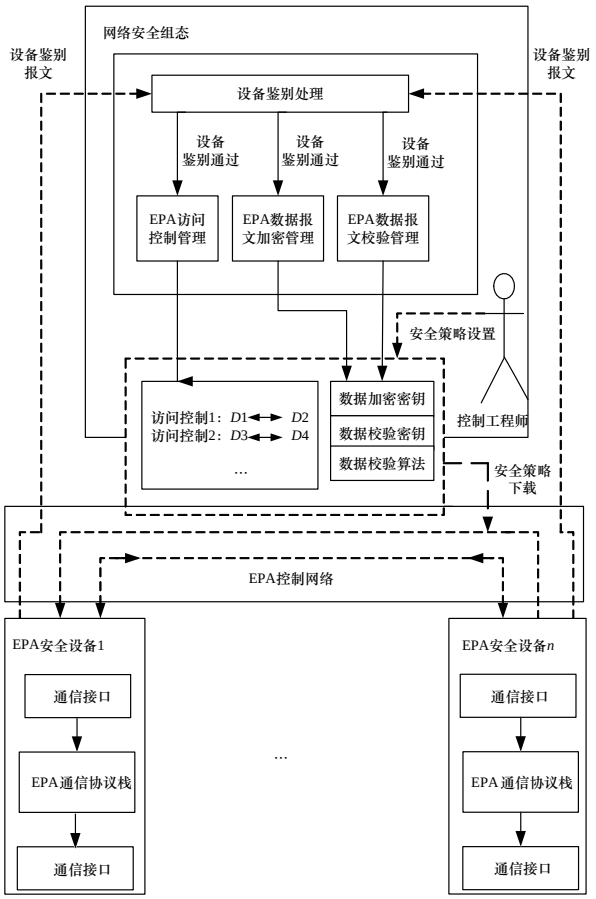


**图 2　EPA 网络安全组态的结构**

## 3　EPA网络安全组态的实现

### 3.1　EPA设备鉴别处理

EPA 设备通过设备鉴别服务进行鉴别。发送方在发送设备鉴别服务时，使用 MD5 算法对 DeviceID、时间戳和 SecurityID 所组成的 8 位位组串进行摘要。摘要值作为鉴别码 Authentication Code 与设备的 Device ID, Active IP Address、时间戳等共同构成设备鉴别报文一起发送。发送的数据具体结构如下：

```
typedef struct
{
unsigned char DeviceID[32]; //本地设备 ID
Unsigned32 secs;//时间戳 1
Unsigned32 nasecs;//时间戳 2
Unsigned char AuthenticatedYard[16]; //本地设备鉴别码
Unsigned32 Active IPAddress;//IP 地址
} EM_DEVICEAUTHENTICATION;
```

组态软件作为鉴别服务的接收方，在收到设备鉴别服务时，根据设备鉴别报文内的 DeviceID 字段查找设备描述文件，从其中读取 SecurityID。SecurityID, DeviceID 和从设备鉴别报文中取得的时间戳共同组成 8 位位组，采用 MD5 算法进行摘要获得正确鉴别码。若从报文中获取的鉴别码与正确鉴别码一致，则向发送端发送设备鉴别确认服务，设置设备鉴别状态为已通过，允许对其组态，并写入通过鉴别的时间戳，否则认为设备不可信，拒绝对其进行组态。

### 3.2　EPA设备访问控制管理

EPA 设备访问控制管理应用于使用 EPA 协议对功能块和管理信息库中的变量对象、域对象、事件对象的存取访问。依照不同的 SRL，安全网关将 PCN 保护起来，防止来自外部网络的威胁。EPA 设备访问控制管理的基本任务：防止未授权，进入 EPA 系统和授权的用户对系统资源的非法使用。

根据 EPA 网络安全规范，在组态软件中，访问控制对象定义如下：

```
class CAcceptControlObj : public CParamStruct{
Private:
Unsigned16　m_ObjectID;//在管理信息库中索引
Unsigned16　m_LocalAppID;//本地功能块标识
Unsigned16　m_LocalObjectID;//本地变量索引
Unsigned16　m_RemoteAppID;//远程功能块标识
Unsigned16　m_RemoteObjectID;//远程变量索引
Unsigned8 m_ServiceOperation;//EPA 服务类型
Unsigned8 m_ServiceRole;//EPA 服务角色
Unsigned32　m_RemoteIPAddress;//远程设备 IP
Unsigned32m_SendTimeOffset;//报文发送时间相对于通信宏//周期起始时间的偏离量
Unsigned8 m_AccessRight;//访问权限
Unsigned8 m_AccessGroup;//访问组
Unsigned16 m_Password;//口令
…成员函数略};
```

EPA 网络安全组态时，组态软件从当前界面上的可视化功能块和连线信息可以获得访问控制列表长度以及 CAcceptControlObj 对象的 m_ObjectID, m_LocalAppID, m_LocalObjectID, m_RemoteAppID, m_RemoteObjectID, m_RemoteIPAddress，而 CAcceptControlObj 对象的 m_AccessRight, m_AccessGroup, m_Password 从安全组态设置窗口来获取。

由于EPA标准和EPA安全规范中规定的数据格式与组态软件中使用的数据格式有所差异，因此需要经过编译，将访问控制列表长度和所有 CAcceptControlObj 对象中的信息通过 EPAWrite 服务下载到安全设备中。

### 3.3　EPA数据报文加密管理

EPA 报文发送方利用加密密钥 EPAKey，通过用异或算法或者 AES 算法对报文加密。然后将加密后的用户数据作为报文体加在安全报文头后交 EPA 应用实体发送。接收方用安全报文头中的时间戳得到解密密钥 EPAKey，运用该密钥 EPAKey 对接收到的用户报文进行异或算法或者 AES 算法解密，得到解密后的用户数据，并将用户数据上传。

EPA 安全设备内都维护着一张密钥表，组态软件在对 EPA 安全设备组态时，必须为整个网段内的 EPA 安全设备下载密钥表，否则 EPA 安全设备将会因为没有匹配的密钥而不能实现相互通信。密钥表是从组态软件中获取 16 个 4 位整型的随机数，然后将其打包生成。组态软件需要设置密钥表管理对象中的当前使用密钥在密钥表内的偏移量，该偏移量通过安全组态设置窗口设置。

### 3.4　EPA数据报文校验管理

发送方选择校验密钥，利用该校验密钥对用户数据进行处理得到校验码，将用户数据与校验码一起作为报文体交 EPA 应用实体发送。接收方根据选择的校验密钥，运用此校验密钥与接收到的用户数据进行处理得到新校验码。将此新校验码与接收报文中的校验码进行比较，若完全相同则确定消息合法并接受数据包，否则丢弃该数据包，并根据 ServiceID 决定是否返回负响应。

组态软件对数据校验的处理主要有 2 个方面：

(1)校验密钥管理：组态软件可以设置动态获取校验密钥和静态获取校验密钥。动态获取校验密钥是根据本地时间戳得到校验密钥，静态获取校验密钥在组态软件中获取 16 个 4 位整型的随机数，然后将其打包生成的同时，组态软件要设置校验密钥表，管理对象中的当前使用校验密钥在校验密钥表内的偏移量。

(2)校验算法管理：EPA 设备维护校验算法表，校验算法表中保存着各种校验算法处理函数的函数指针。组态软件在对 EPA 安全设备组态时要选择当前校验算法在校验算法表中的偏移量。

## 4 EPA网络安全组态实例

本 EPA 网络安全组态实例利用 EPA 组态软件对 EPA 网络中的安全设备进行鉴别，对合法的安全设备进行功能块组态并设置访问控制权限、密钥、校验算法，实现 EPA 安全设备之间的通信。

### 4.1 EPA安全设备上线

EPA 网络中所有的安全设备都需要在 EPA 组态软件进行上线处理，上线处理的目的：

(1)构造安全设备在 EPA 组态软件中映射的信息结构；

(2)通过设备鉴别来鉴定 EPA 安全设备的合法性。

### 4.2 EPA设备安全组态

EPA 组态软件对所有通过设备鉴别的合法安全设备进行链路组态、访问控制设置、数据报文加密密钥设置、数据报文检验密钥和算法设置。对于没有通过设备鉴别的非法安全设备，EPA 组态软件拒绝对其进行链路组态和安全设置。

EPA 合法安全设备组态如图 3 所示。

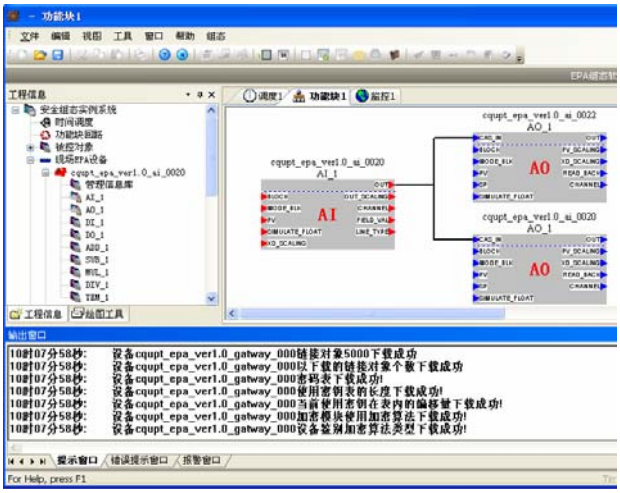

**图 3 EPA 合法安全设备组态**

图 4 为网络安全组态设置窗口。

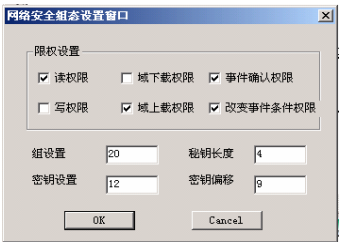


**图 4 网络安全组态设置窗口**

在组态完成后，EPA 安全设备中的访问控制链表、加密密钥、校验密钥如图 5 所示。

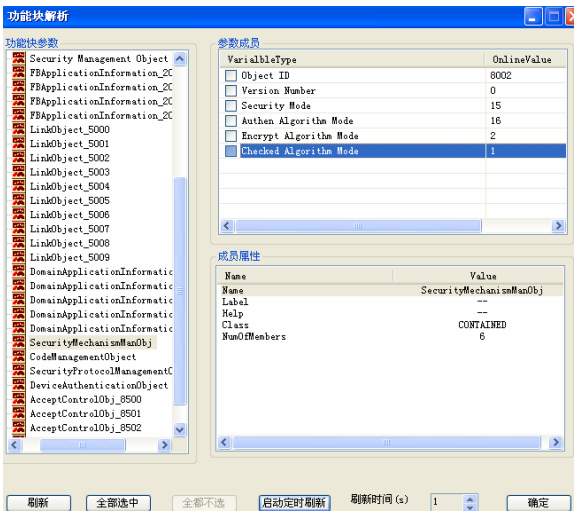


**图 5 EPA 安全设备中的安全数据信息**

### 4.3 安全设备通信测试

安全设备通信测试具体包括：

(1)访问控制测试。测试访问控制时，使用 EPA 组态软件模拟未经授权的应用进程发送变量写报文，由于 EPA 设备组态未制定安全设备与该应用进程间的通信关系，因此该访问会被 EPA 安全设备拒绝，网络监控计算机接收到变量写负响应报文。访问控制措施安全功能测试结果如图 6 所示。测试结果为 EPA 组态软件运行的 EPA 协议栈模拟软件接收到变量读负响应报文，错误描述为访问控制权限不存在。结果证明，访问控制措施可以保护 EPA 数据免于为授权的访问，保证 EPA 系统信息安全。


**图 6 访问控制措施安全功能测试结果**

(2)数据加密与校验测试。测试数据加密和数据校验措施的目的是确定数据加密和数据校验过程是完全可逆的，并且不会对原数据造成影响。测试数据加密和数据校验过程首先从 EPA 安全设备发送 EPA 安全变量写报文，然后从网络中抓取该报文，分析报文内容，最后在目的端解析报文。图 7 为网络中的 EPA 安全变量写报文密文。

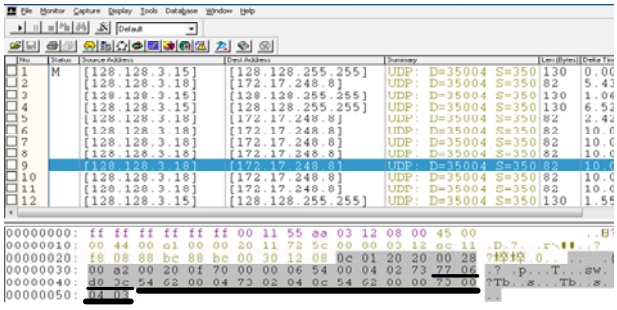

**图 7 网络中的 EPA 安全变量写报文密文**

(下转第 233 页)