DOI：10.13890/j.issn.1000-128X.2026.02.101

# 动车组网络安全风险评估及防范技术研究

董敬超，李　辉，崔红月
（中车唐山机车车辆有限公司 产品研发中心，河北 唐山 063035）

**摘　要：**随着动车组智能化水平的不断提升，车载网络逐渐采用商用信息化组件，并逐步开放与地面系统的数据交互接口。这一发展趋势在提升动车组运营效率的同时，也显著增加了车辆运行安全和数据泄漏的风险。为有效应对上述挑战，文章提出一种面向网络安全等级保护要求的动车组网络安全风险评估方法。首先，针对动车组网络的特点，基于层次分析法构建不同应用场景下的风险因素耦合关系模型，并对风险要素进行权重评估；在此基础上，运用改进的模糊综合评价法，对动车组网络的安全风险水平进行量化评估。该方法旨在为动车组网络提供一套科学、精准且可操作的安全风险评估体系，以提升其整体安全防护能力。

**关键词：**动车组；高速列车；网络安全风险评估；安全等级保护；模糊综合评价

**中图分类号：**U292.91+4；TN915.08　　**文献标志码：**A　　**文章编号：**1000-128X(2026)04-0066-09

## 0　引言

随着动车组智能化与数字化进程的加速推进，其车载网络架构已深度整合了车载信息、地面运营数据、维护系统及轨旁设备等多源信息。高度互联互通在提升运营效率的同时，也显著扩大了系统的攻击面，使得跨域数据泄漏、协议漏洞利用及恶意代码渗透等新型安全威胁日益严峻，对行车安全与数据完整性构成了直接挑战。因此，亟须建立一套科学、有效的安全风险评估体系，为动车组网络的安全防护提供精准依据。然而，当前国内动车组网络系统缺乏权威且适用的安全水平量化评价方法。虽然 GB/T 22239—2019《信息安全技术 网络安全等级保护基本要求》（以下称等级保护 2.0）为一般信息系统提供了安全评价框架，但其通用性要求难以充分反映动车组网络特有的拓扑结构、实时性约束、物理环境耦合性以及安全功能优先级的差异性，直接套用该标准进行风险评估存在显著局限性[1]。

为克服上述不足，本文提出一种适配于动车组网络特点的网络安全风险评估方法。该方法以等级保护 2.0 为基础[2]，结合动车组特定需求重构关键指标并调整权重。在评估技术上，融合层次分析法[3]（analytic hierarchy process， AHP）与模糊综合评价法[4]，通过 AHP 科学确定指标权重，利用模糊评价处理评估中的模糊性与不确定性，从而构建一套针对性更强、可量化、可操作的动车组网络安全风险评估模型，为提升防护的精准性和有效性提供技术支撑。

## 1　动车组网络系统安全风险分析

随着动车组网络向智能化和互联互通方向发展，其受攻击面显著扩大，面临多维度安全威胁。本文基于等级保护 2.0 保护的核心框架，系统分析动车组网络在各防护域面临的关键安全风险及其成因，并明确相应的安全防护需求。

### 1.1　安全区域边界风险分析

动车组网络内部通常包含多个功能子系统，这些子系统之间以及动车组网络与外部网络之间都需要进行受控的数据交换。核心风险在于非授权或恶意的跨边界数据流动，可能导致敏感数据泄漏，使恶意代码或攻击流量通过边界薄弱点侵入关键子系统。因此，安全区域边界防护的核心需求在于建立并维持可控的

**通信作者：**董敬超，男，高级工程师，主要从事列车网络控制系统的研发和设计；E-mail: tsdongjingchao@163.com

**引用格式：**董敬超，李辉，崔红月．动车组网络安全风险评估及防范技术研究[J]. 机车电传动，2026(4): 66-74.DOI:10.13890/j.issn.1000-128X.2026.02.101.

**Citation：**DONG Jingchao, LI Hui, CUI Hongyue. Research on cybersecurity risk assessment and protection technologies for electric multiple units[J]. Electric drive for locomotives,2026(4): 66-74.DOI:10.13890/j.issn.1000-128X.2026.02.101.

访问边界。通过部署边界防火墙等设备，对所有跨越安全域的数据流实施严格的访问控制策略；同时，强化边界防护设备安全管理，实现权限控制动态调整策略，建立基于终端授权认证的网络准入控制机制。

### 1.2　安全通信网络安全风险分析

通信网络作为承载动车组各业务系统数据交互的基础，核心风险包括网络资源耗尽、网络监听与篡改。为此，需依据业务功能和安全等级实施网络分区策略，采用虚拟局域网技术分离不同安全域，将关键业务部署在安全等级高的域，敏感数据传输需采用强加密协议。

### 1.3　安全计算环境风险分析

网络设备、服务器、终端等计算节点是攻击者最终的目标，核心风险在于非授权访问、恶意代码感染、数据泄漏与篡改以及远程管理风险。因此，需实施严格的身份认证机制，要求采用高复杂度口令并定期更换，远程管理采用加密协议，并遵循最小权限原则配置权限，关闭非必需服务和端口，全面加密保护敏感数据和日志。

### 1.4　安全管理中心风险分析

面对分布式部署的网络设备、安全设备和终端，运维人员难以实时掌握全网设备运行状态、安全事件分布及威胁发展趋势。因此，安全管理中心建设的核心需求是实现安全能力的集中化、可视化和高效响应。通过部署相关专业的入侵防护系统，对高速列车网络中发生的各类安全事件进行识别、报警和分析，确保相关安全事件得到及时发现和及时处置。

## 2　动车组网络系统安全风险评估

### 2.1　网络系统风险评估模型

基于动车组网络风险分析，其安全评估流程如图1所示。首先，以等级保护2.0框架为核心，确立安全评估目标与综合评价体系；其次，采用层次分析法，构建以列车停车、干扰驾驶与数据泄漏为准则层的分析模型，结合标度法生成判断矩阵并计算权重参数；最后，在模糊综合评价阶段，基于评语集构建隶属度矩阵，并通过权重参数与矩阵的合成运算量化风险等级，最终得到动车组网络系统的安全风险评价。

根据高速铁路网络系统安全威胁场景分析，将网络系统风险分成不同层次的要素，构成递阶层次结构，如图2所示。

### 2.2　确定各层元素权重

建立层次结构后，将上一层级作为约束条件，比较下一层级中各要素的相对重要性，如表1所示，采用

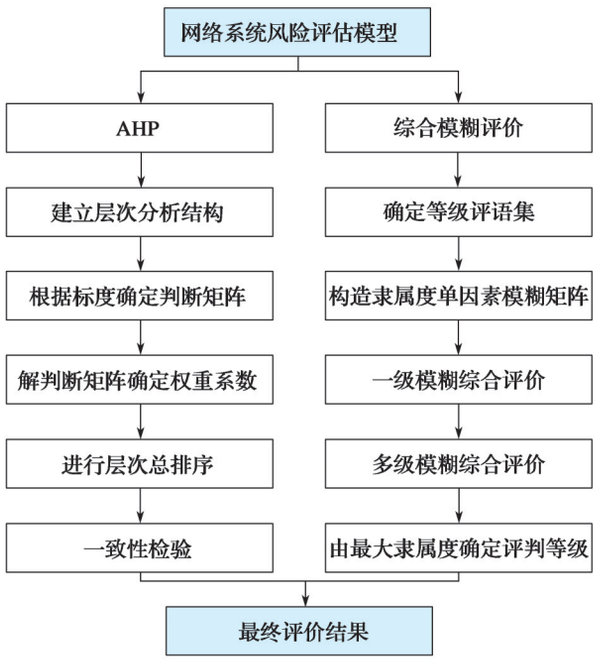



图1　风险评估流程

Fig. 1　Risk assessment process

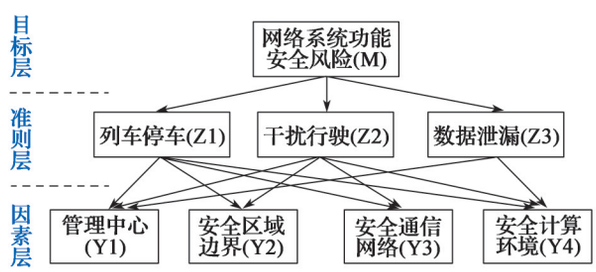



图2　风险层次分析结构

Fig. 2　Analytic hierarchy structure for risks

1~9标度法来构造判断矩阵。

表1　1~9标度表示法

Table 1　Scale notation for 1–9

| 重要性标度 | 含义 |
|---|---|
| 1 | 表示两个元素相比，具有同等重要性 |
| 3 | 表示两个元素相比，前者比后者稍微重要 |
| 5 | 表示两个元素相比，前者比后者明显重要 |
| 7 | 表示两个元素相比，前者比后者强烈重要 |
| 9 | 表示两个元素相比，前者比后者极端重要 |
| 2, 4, 6, 8 | 表示上述判断的中间值 |
| 倒数 | 若元素 $i$ 与元素 $j$ 的重要性之比为 $b_{ij}$，则元素 $j$ 与元素 $i$ 的重要性之比为 $1/b_{ij}$ |

以准则层中列车停车（Z1）作为约束条件，安全边界被识别为动车组网络系统的首要防护目标。传统列车系统因相对封闭性，长期未遭受严重网络攻击；然而，随着智能化与以太网技术的应用，系统开放性显著增加，边界防护成为防护的重点。其次，安全通信对列车停驶风险具有关键影响，例如通过虚拟局域网隔离关键网络（如乘客信息系统与核心控制网），可确保局部攻击不扩散至行车功能。对因素层中Y1~Y4

的4类威胁场景的重要程度按照标度法计算得到判断矩阵表如表2。

表2 1~9判断矩阵表

Table 2 judgment matrix for 1–9

| 项目 | 管理中心 | 安全边界 | 安全通信 | 安全计算 |
|---|---|---|---|---|
| 管理中心 | 1 | 1/5 | 1/3 | 1/3 |
| 安全边界 | 5 | 1 | 3 | 3 |
| 安全通信 | 3 | 1/3 | 1 | 3 |
| 安全计算 | 3 | 1/3 | 1/3 | 1 |

判断矩阵$\boldsymbol{\beta}_{Z1}$为

$$\boldsymbol{\beta}_{Z1}=\begin{bmatrix}1 & 1/5 & 1/3 & 1/3\\ 5 & 1 & 3 & 3\\ 3 & 1/3 & 1 & 3\\ 3 & 1/3 & 1/3 & 1\end{bmatrix} \tag{1}$$

利用判断矩阵计算在顶层Z1的约束下，准则层Y1、Y2、Y3和Y4的权重，计算权重系数的方法一般分为和积法、几何平均法和特征值法，本文采用和积法计算权重，该方法的步骤如下[5]：

①按照式(2)将判断矩阵的每一列元素做归一化处理。

$$\bar{b}_{ij}=\frac{b_{ij}}{\sum_{i=1}^{n}b_{ij}},\quad i,j=1,2,\cdots,n \tag{2}$$

式中：$b_{ij}$为判断矩阵第$i$行、第$j$列的元素；$n$为矩阵的维数。

②按照式(3)将归一化的矩阵$\bar{\boldsymbol{\beta}}_{Z1}$按行相加。

$$\boldsymbol{W}_{Z1}=\begin{bmatrix}w_1 & w_2 & \cdots & w_i\end{bmatrix}^{\mathrm{T}} \tag{3}$$

式中：$w_i$表示$\bar{b}_{ij}$按行相加，$w_i=\sum_{j=1}^{n}\bar{b}_{ij}\ (i=1,2,\cdots,n)$。

③对向量$\boldsymbol{W}_{Z1}$进行归一化得到$\bar{\boldsymbol{W}}_{Z1}$，即为判断矩阵$\boldsymbol{\beta}_{Z1}$的权重系数向量即特征向量。

为了避免判断矩阵中的数值可能出现矛盾的地方，要对判断矩阵进行一致性检验，检验步骤如下：

①按照式(4)计算判断矩阵最大特征值的近似值。

$$\lambda_{\max}=\frac{1}{n}\sum_{i=1}^{n}\frac{\left(\boldsymbol{\beta}_{Z1}\bar{\boldsymbol{W}}_{Z1}\right)_i}{\left(\bar{\boldsymbol{W}}_{Z1}\right)_i} \tag{4}$$

式中：$n$为矩阵的维数；$\boldsymbol{\beta}_{Z1}$为判断矩阵；$\bar{\boldsymbol{W}}_{Z1}$为特征向量。

计算可得最大特征值$\lambda_{\max}=4.201$。

②按照式(5)计算并检验矩阵一致性指标C.I值$A_{C.I}=0.067$。

$$A_{C.I}=\frac{\lambda_{\max}-n}{n-1} \tag{5}$$

③对大量随机矩阵的C.I取平均值得到4阶矩阵平均一致性指标$A_{R.I}=0.882$，按照式(6)计算随机一致性比率$A_{C.R}=0.077$。

$$A_{C.R}=\frac{A_{C.I}}{A_{R.I}} \tag{6}$$

当$A_{C.R}<0.1$时，具有较好的一致性，证明矩阵无须重新调整。

为了验证上述计算的正确性，采用SPSSPRO在线分析工具对判断矩阵$\boldsymbol{\beta}_{Z1}$进行AHP分析计算，结果如表3所示。研究团队对表3数据进行对比，发现两种计算结果一致，从而验证了上述计算的正确性。

表3 Z1约束下AHP层次分析结果

Table 3 AHP analytic hierarchy process results under Z1 constraints

| 项目 | 特征向量 | 权重值 | 最大特征根 | C.I值 |
|---|---|---|---|---|
| 管理中心 | 0.307 | 7.682% | 4.201 | 0.067 |
| 安全边界 | 2.005 | 50.115% | | |
| 安全通信 | 1.052 | 26.297% | | |
| 安全计算 | 0.636 | 15.909% | | |
| 一致性检验结果 | | | | |
| 最大特征根 | C.I值 | R.I值 | C.R值 | 一致性检验结果 |
| 4.201 | 0.067 | 0.882 | 0.076 | 通过 |

以此类推，分别计算准则层Z2、Z3和目标层M的AHP分析结果。

以Z2影响行车作为约束条件，网络边界的安全应该还是最重要的，其能够保证列车关键网络免受攻击，其次安全计算环境也比较重要，例如乘客信息系统网络遭受到了攻击，导致旅客指引信息发生错误，将导致乘客的混乱，影响行车。对因素层中Y1~Y4的4类威胁场景的重要程度按照标度法计算得到判断矩阵表4和分析结果表5。

表4 Z2判断矩阵表

Table 4 Z2 judgment matrix

| 项目 | 管理中心 | 安全边界 | 安全通信 | 安全计算 |
|---|---|---|---|---|
| 管理中心 | 1 | 1/3 | 3 | 1 |
| 安全边界 | 3 | 1 | 3 | 3 |
| 安全通信 | 1/3 | 1/3 | 1 | 1/3 |
| 安全计算 | 1 | 1/3 | 3 | 1 |

表5 Z2约束下AHP层次分析结果

Table 5 AHP analytic hierarchy process results under Z2 constraints

| 项目 | 特征向量 | 权重值 | 最大特征根 | C.I值 |
|---|---|---|---|---|
| 管理中心 | 0.842 | 21.042% | 4.155 | 0.052 |
| 安全边界 | 1.925 | 48.125% | | |
| 安全通信 | 0.392 | 9.792% | | |
| 安全计算 | 0.842 | 21.042% | | |
| 一致性检验结果 | | | | |
| 最大特征根 | C.I值 | R.I值 | C.R值 | 一致性检验结果 |
| 4.155 | 0.052 | 0.882 | 0.059 | 通过 |

以Z3数据泄漏作为约束条件，首先安全计算环境较为重要，包括数据的加密，数据的存储等要求，即便是伪基站的窃取技术也能够完美地防范；其次安全边界也相对重要，在安全边界中要求访问的授权，能够有效地阻止窃取访问。应该对因素层中Y1~Y4的4

类威胁场景的重要程度按照标度法计算得到判断矩阵如表6和分析结果如表7。

表6　Z3判断矩阵表

Table 6　Z3 judgment matrix

| 项目 | 管理中心 | 安全边界 | 安全通信 | 安全计算 |
|---|---|---|---|---|
| 管理中心 | 1 | 5 | 3 | 5 |
| 安全边界 | 1/5 | 1 | 3 | 3 |
| 安全通信 | 1/5 | 3 | 1 | 1 |
| 安全计算 | 1/3 | 3 | 1 | 1 |

表7　Z3约束下AHP层次分析结果

Table 7　AHP analytic hierarchy process results under Z3 constraints

| 项目 | 特征向量 | 权重值 | 最大特征根 | C.I值 |
|---|---|---|---|---|
| 管理中心 | 2.238 | 55.948% | 4.115 | 0.038 |
| 安全边界 | 0.307 | 7.667% | | |
| 安全通信 | 0.766 | 19.154% | | |
| 安全计算 | 0.689 | 17.231% | | |
| 一致性检验结果 | | | | |
| 最大特征根 | C.I值 | R.I值 | C.R值 | 一致性检验结果 |
| 4.115 | 0.038 | 0.882 | 0.044 | 通过 |

M作为约束条件，对因素层中Z1~Z3的3类准则的重要程度按照标度法计算得到判断矩阵如表8和分析结果表9。

表8　M判断矩阵表

Table 8　M judgement matrix

| 项目 | 列车停车 | 干扰行驶 | 数据泄漏 |
|---|---|---|---|
| 列车停车 | 1 | 3 | 5 |
| 干扰行驶 | 1/3 | 1 | 3 |
| 数据泄漏 | 1/5 | 1/3 | 1 |

表9　M约束下AHP层次分析结果

Table 9　AHP analytic hierarchy process results under M constraints

| 项目 | 特征向量 | 权重值 | 最大特征根 | C.I值 |
|---|---|---|---|---|
| 列车停车 | 1.900 | 63.333% | 3.039 | 0.019 |
| 干扰行驶 | 0.782 | 26.050% | | |
| 数据泄漏 | 0.318 | 10.617% | | |
| 一致性检验结果 | | | | |
| 最大特征根 | C.I值 | R.I值 | C.R值 | 一致性检验结果 |
| 3.039 | 0.019 | 0.525 | 0.037 | 通过 |

根据上文所述，计算各约束下的权重值系数分别为（向量元素省略%符号）：$\bar{\boldsymbol{W}}_{Z1}$、$\bar{\boldsymbol{W}}_{Z2}$、$\bar{\boldsymbol{W}}_{Z3}$、$\bar{\boldsymbol{W}}_{M}$，通过上述的向量，根据式(7)计算出目标M对场景Y的权重向量$\boldsymbol{W}_{M\text{-}Y}$。

$$\boldsymbol{W}_{M\text{-}Y}=\left[\bar{\boldsymbol{W}}_{Z1}\quad\bar{\boldsymbol{W}}_{Z2}\quad\bar{\boldsymbol{W}}_{Z3}\right]\times\bar{\boldsymbol{W}}_{M}\tag{7}$$

随后，进行归一化处理可以得到$\bar{\boldsymbol{W}}_{M\text{-}Y}=[0.162\quad0.451\quad0.212\quad0.174]^{T}$，$\bar{\boldsymbol{W}}_{M\text{-}Y}$权重向量元素依次对应安全中心、安全边界、安全通信和安全计算环境，从结果中可以看出安全边界占比较大，其次是安全通信。

## 2.3　确定评价集合和隶属度矩阵

将影响因素构成评估因素集$U$，得到$U$={管理中心，安全边界，安全通信，安全计算环境}。根据威胁场景的严重程度，设定安全等级的评语集为{较低，低，中等，高，较高}。

研究团队采用通用漏洞评分系统（common vulnerability scoring system, CVSS）方法[6]，从两方面进行评估，一方面是影响度反映漏洞被成功利用所造成的直接后果，包括机密性、完整性、可用性；另一方面针对漏洞的可利用性和技术手段难易度，主要考虑攻击路径、复杂度、权限要求等指标，如表10所示。

表10　通用漏洞评分方法

Table 10　Common vulnerability scoring methodology

| 评价方向 | 指标 | 威胁程度 | 分值 |
|---|---|---|---|
| 影响度 | 机密性（$C$） | 不受影响/部分/完全 | 0/0.7/1.0 |
| | 完整性（$I$） | 不受影响/部分/完全 | 0/0.7/1.0 |
| | 可用性（$A$） | 不受影响/部分/完全 | 0/0.7/1.0 |
| 可利用度 | 攻击途径（$A_V$） | 本地/远程 | 0.7/1.0 |
| | 攻击复杂度（$A_C$） | 高/中/低 | 0.6/0.8/1.0 |
| | 权限要求（$P_R$） | 需要/不需要 | 0.6/1.0 |

按照式(8)计算单个漏洞的分值。

$$X=10A_VA_CP_R\left(Cm_C+Im_I+Am_A\right)\tag{8}$$

式中：$A_V$为共计途径权值；$A_C$为攻击复杂度权值；$P_R$为权限要求权值；$m_C$、$m_I$、$m_A$分别表示机密性、完整性、可用性的权值。

研究团队根据表11所示漏洞严重程度，统计不同严重程度的占比，并以此确定评估因素集$U$对评语集$V$的隶属度矩阵。

表11　漏洞严重程度分级

Table 11　Vulnerability severity classification

| 分值区间 | [0,2) | [2,4) | [4,6) | [6,8) | [8,10] |
|---|---|---|---|---|---|
| 风险等级 | 较低 | 低 | 中等 | 高 | 较高 |

研究团队采用上述对风险的分析方法，结合上文的威胁场景分析和风险评估模型，分析得出网络控制系统容易出现的安全问题共34项，其中安全计算环境问题17项。结合CVSS评分方法计算得出安全问题中，风险较低6个，风险低5个，风险中等3个，风险高3个，风险较高0个，形成安全计算环境的风险评估向量[6 5 3 3 0]，以此类推得到子系统中其他威胁场景类别的风险评估向量。将4个场景类别的风险评估向量组成隶属度矩阵$\boldsymbol{R}$，如式(9)所示。式(9)的第一行为管理中心评估向量，第二行为安全边界评估向量，第三行为安全通信评估向量，第四行为安全计算环境评估

向量。

$$\boldsymbol{R}=\begin{bmatrix}0&3&4&6\\2&4&0&5\\1&1&0&3\\0&2&0&3\\0&0&0&0\end{bmatrix} \tag{9}$$

### 2.4 风险评价

按照式(10)计算列车组网络安全风险综合评价向量。

$$\boldsymbol{W}_{\mathrm{R}}=\bar{\boldsymbol{R}}\times\bar{\boldsymbol{W}}_{\mathrm{M\text{-}Y}} \tag{10}$$

式中：$\bar{\boldsymbol{R}}$表示隶属度矩阵归一化；$\bar{\boldsymbol{W}}_{\mathrm{M\text{-}Y}}$表示$\boldsymbol{R}$对应的权重向量。

研究团队对$\bar{\boldsymbol{R}}$和$\bar{\boldsymbol{W}}_{\mathrm{M\text{-}Y}}$进行模糊合成运算，随后对$\boldsymbol{W}_{\mathrm{R}}$进行归一化处理后可以得到$\bar{\boldsymbol{W}}_{\mathrm{R}}=[0.320\quad 0.435\quad 0.126\quad 0.118\quad 0]^{\mathrm{T}}$。

由$\bar{\boldsymbol{W}}_{\mathrm{R}}$结果可知，在目标层的评价结果中，32.0%可能属于风险较低，43.5%可能属于风险低，12.6%可能属于风险中等，11.8%可能属于风险高，0%可能属于风险较高。根据最大隶属度原则，动车组网络系统功能安全风险的风险等级为中风险，评估如图3所示。

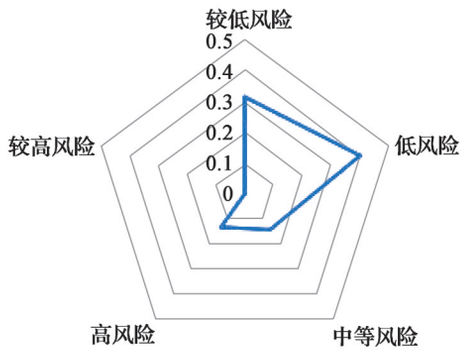



图3 动车组网络系统风险评估图

Fig. 3 Risk assessment diagram of EMU network system

## 3 动车组网络安全系统方案

### 3.1 安全框架和拓扑设计

基于对动车组网络系统风险的深入分析，并依据等级保护2.0的要求，研究团队提出了涵盖安全管理中心、安全计算环境、安全区域边界和安全网络通信4个关键方面的动车组网络系统安全框架方案，具体如图4所示。

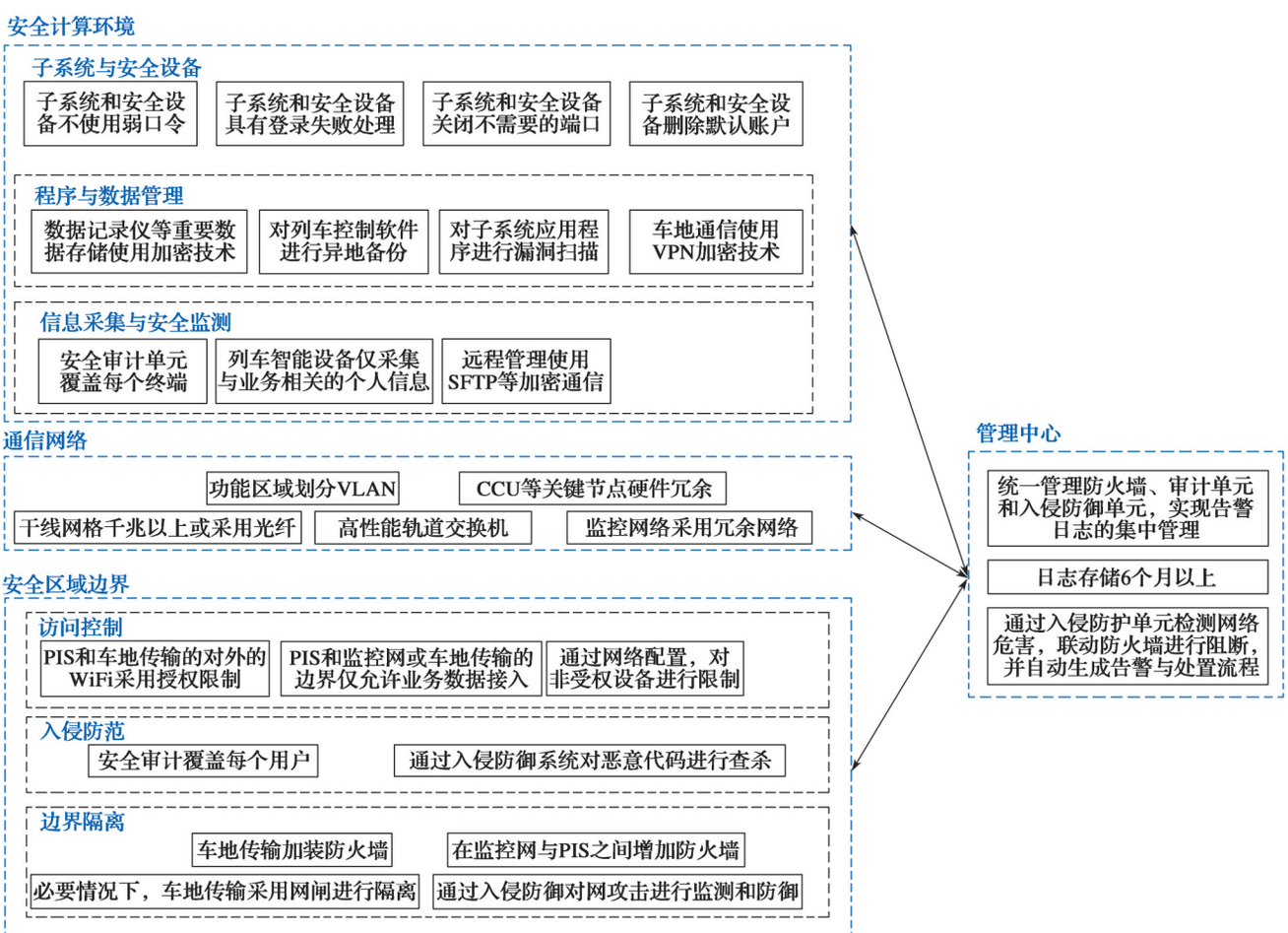



图4 动车组网络系统安全框架

Fig. 4 Security framework of EMU network system

该方案在多项关键安全要求上已达到等保三级水平，可显著降低网络系统遭受安全威胁的风险概率[7]。

为实现上述安全框架要求，提升动车组整体网络安全防护能力，需在现有网络设备（终端、交换机）安全配置优化的基础上，对网络拓扑结构进行针对性调整。主要调整措施包括：在列车内部网络（车载网）与车地通信网络边界部署防火墙，并在全网范围内部署网络监测审计与日志审计单元，如图5所示。

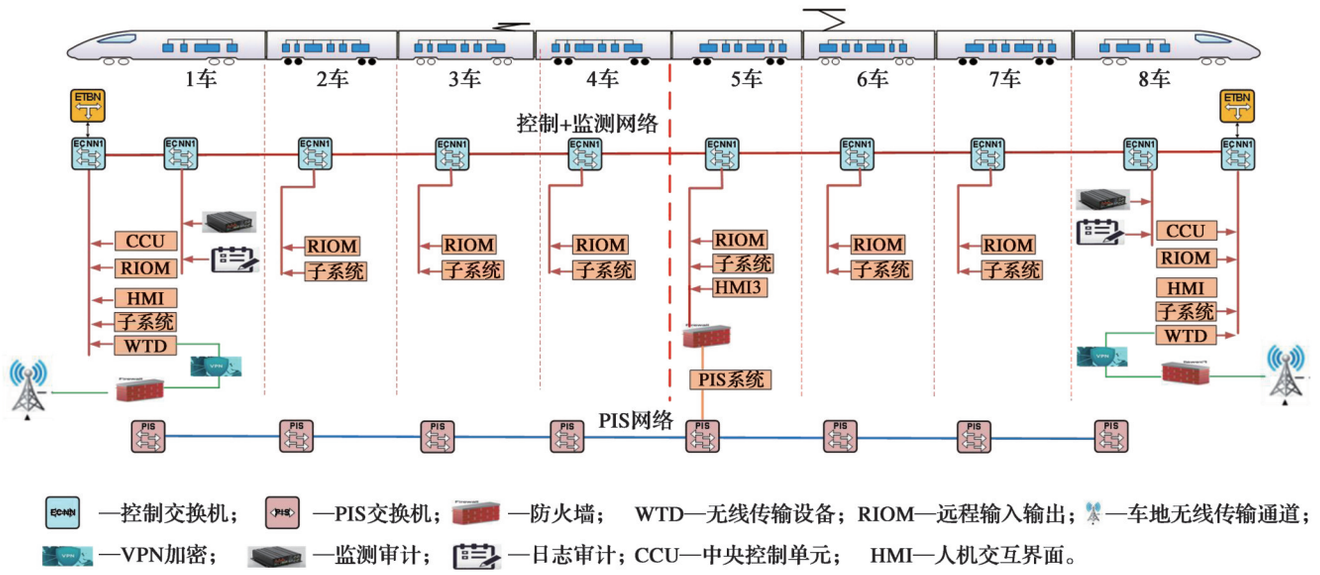



图5　动车组安全网络系统拓扑结构

Fig. 5　Topology of EMU security network system

## 3.2　关键安全设备功能设计

研究团队针对安全框架的核心防护需求，对车载防火墙、网络监测审计单元、日志审计单元及VPN加密模块等关键设备进行了详细的功能设计，这些设备协同工作，共同构建纵深防御体系。

鉴于旅客信息系网络存在外部接口，在车载控制网与乘客信息系统网络间串行部署车载防火墙至关重要。如图6所示，该防火墙可有效阻断外部对列车内部网络的非授权访问与登录，并对异常报文、异常流量及外部入侵行为实施实时监测与防护，满足安全框架中关于安全边界防护的要求。其核心功能包括访问控制、应用白名单、心跳监测、网络地址转换、会话限制及状态监测等。

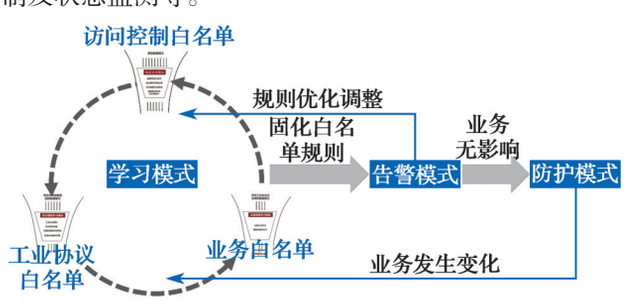



图6　防火墙工作模式

Fig. 6　Firewall working mode

监测审计单元通过智能学习机制，构建基于通信协议及关键字段的正常通信行为“白名单”基线模型。对偏离基线的通信行为进行告警，实现对常见及新型网络攻击的有效检测。同时，该单元能够检测并识别网络中的未授权接入设备，完整记录列车异常网络通信流量，为后续安全事故的调查取证提供关键技术支持，满足安全框架中安全计算环境对检测与防护的要求。具体功能涵盖列车网络异常监测、网络攻击检测、无流量事件检测、关键事件检测、日志告警上报及生命信号发送等。

车载日志审计单元负责对列车内部各类终端设备（主机、网络设备、安全设备）产生的日志进行采集、范式化处理与集中管理。提供百余种关联分析规则，辅助运维人员快速精准地识别安全事件与违规行为，大幅提升运维效率。如图7所示，支持一键生成安全运维报告，简化日常日志分析与报告编制工作，满足安全框架中安全管理中心对日志审计的要求。核心功能包括数据采集、数据解析、告警响应、日志长期留存、日志深度分析及综合安全审计等。

VPN加密模块采用IPSec协议作为全球通用的VPN安全标准，确保不同厂商设备间的互操作性，如图8所示，IPSec协议通过封装安全载荷（ESP）提供数据机密性（加密），并通过认证头（AH）或ESP认证提供数据完整性与源认证，保障网络通信报文的传输安全。建议密钥算法采用国密SM4标准，以满足安全框架中安全计算环境对数据安全管理的要求。

## 3.3　网络安全补偿评估

一般情况下，高速列车网络系统安全等级越高成本也越高，例如对CCU、TCU等子系统进行程序的安全扫描将会增加成本；增加网闸会导致成本增




图7　车载日志审计管理界面

Fig. 7　Onboard log audit management interface




图8　VPN配置界面

Fig. 8　VPN configuration interface

加、通信数据格式僵化等问题。因此，对于一般要求的车辆可以考虑在资金和项目研发周期允许范围内进行安全防护的设计；同时考虑前文对安全影响因素权重的分析，建议在列车网络系统中增加防火墙、网络审计、VPN加密等功能，处置弱口令、默认账户和默认端口等问题，划分虚拟局域网来区分网络安全区域等，经过上述安全问题的补偿后，得到隶属度矩阵$\boldsymbol{R}'$如式(11)所示，根据2.4节重新计算得到列车组网络安全风险综合评价向量$\boldsymbol{W}_R'=[0.659\quad 0.154\quad 0.078\quad 0.107\quad 0]^{\mathrm{T}}$。

$$\boldsymbol{R}'=\begin{bmatrix}0 & 6 & 3 & 12\\ 0 & 1 & 1 & 3\\ 0 & 1 & 0 & 2\\ 0 & 2 & 0 & 0\\ 0 & 0 & 0 & 0\end{bmatrix} \tag{11}$$

补偿后目标层的评价结果：65.9%可能属于风险较低，15.4%可能属于风险低，7.8%可能属于风险中等，10.7%可能属于风险高，0%可能属于风险较高。根据最大隶属度原则，动车组网络系统功能安全风险的风险等级为低风险，网络风险评估雷达图如图9所示，与没有补偿之前相比，中高风险的概率明显降低。

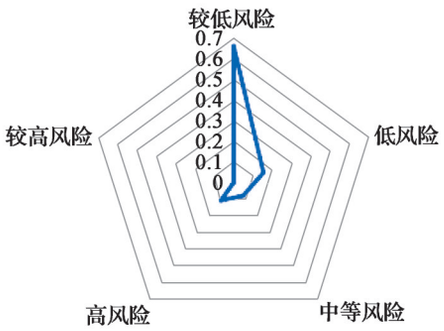



图 9　补偿后的网络系统安全风险评估图

Fig. 9　Security risk assessment of network system after compensation

## 4　结论

本文以某型号动车组网络系统为研究背景，基于等级保护 2.0 要求，采用模糊综合评估法和层次分析法，对动车组网络系统安全风险进行了量化评估，并提出了相应的安全框架建议和安全补偿措施。通过对补偿前后的安全风险水平进行定量分析和比较，验证了所提措施的有效性，结论如下：

①模糊综合评估法和层次分析法的结合，能够有效处理动车组网络系统安全风险评估中的复杂性和不确定性。

②本文所提出的安全框架建议和安全补偿措施，能够显著降低动车组网络系统的安全风险，提升其整体安全防护能力。

③安全补偿措施的实施步骤明确，具有较强的可操作性和可推广性。

未来研究方向可进一步探索人工智能和机器学习技术在动车组网络安全风险评估中的应用，以实现更智能、更高效的安全防护。

## 参考文献：

[1] 李洪赭, 闫连山, 陈建译, 等. 基于威胁分析的高速铁路信号系统风险评估方法[J]. 西南交通大学学报, 2022, 57(6): 1334-1341.
Li Hongzhe, Yan Lianshan, Chen Jianyi, et al. Risk assessment method of high-speed railway signal systems based on threat analysis[J]. Journal of Southwest Jiaotong University, 2022, 57(6): 1334-1341.

[2] 王荣斌, 吴茵, 周黎辉. 基于云平台的信息安全保障及安全风险评估方法的研究[J]. 网络安全技术与应用, 2017(5): 80-81.
Wang Rongbin, Wu Yin, Zhou Lihui. Research on information security assurance and risk assessment methods based on cloud platforms[J]. Network Security Technology & Application, 2017(5): 80-81.

[3] 龚斯谛, 王磊. 基于 AHP 与信息熵的工控系统信息安全风险评估研究[J]. 工业控制计算机, 2017, 30(4): 11-12.
Gong Sidi, Wang Lei. Cyber security risk assessment for industrial control system based on AHP and information entropy[J]. Industrial Control Computer, 2017, 30(4): 11-12.

[4] Deng X H, Wang R, Xu T. Risk assessment of tunnel portals in the construction stage based on fuzzy analytic hierarchy process[J]. Archives of Civil Engineering, 2018, 64(4): 69-87.

[5] 孙宏才, 田平, 王莲芬. 网络层次分析法与决策科学[M]. 北京: 国防工业出版社, 2011.
Sun Hongcai, Tian Ping, Wang Lianfen. Network analytic hierarchy process and decision science[M]. Beijing: National Defense University Press, 2011.

[6] Mell P, Scarfone K, Romanosky S. Common vulnerability scoring system[J]. IEEE Security & Privacy, 2006, 4(6): 85-89.

[7] 何晶. 城市轨道交通云平台网络安全防护平台方案研究[J]. 都市快轨交通, 2020, 33(5): 17-22.
He Jing. Scheme of network security protection platform for cloud computing platform in urban rail transit[J]. Urban Rapid Rail Transit, 2020, 33(5): 17-22.

# Research on cybersecurity risk assessment and protection technologies for electric multiple units

**DONG Jingchao, LI Hui, CUI Hongyue**

(Product R&D Center, CRRC Tangshan Co., Ltd., Tangshan, Hebei 063035, China)

**Abstract:** With the increasing intelligence of electric multiple units (EMUs), commercial information technology components are gradually adopted for onboard networks, and data interaction interfaces with ground-based systems are gradually opened. While this trend enhances operational efficiency of EMUs, it also significantly elevates risks related to vehicle operational safety and data security. To address these challenges, this paper proposes a cybersecurity risk assessment method for EMUs according to the requirements for classified cybersecurity protection systems. Firstly, based on the characteristics of EMU networks, an analytic hierarchy process (AHP) was applied to model the coupling relationships among risk factors in different application scenarios, and the weight assessment was performed for the risk factors. Secondly, the improved fuzzy comprehensive assessment method was employed to quantitatively assess the security risk levels of EMU networks. The proposed method aims to establish a scientific, precise, and operable security risk assessment framework for EMU networks, thereby enhancing their overall cybersecurity protection capabilities.

**Keywords:** EMU; high speed train; cybersecurity risk assessment; classified cybersecurity protection; fuzzy comprehensive assessment

收稿日期：2024-08-16；修回日期：2025-11-03

责任编辑：钟　锋