业务视角安全模型评估法

Security Model Evaluation Method from Business Perspective

丁　峰（中国联通上海分公司，上海 200050）
Ding Feng（China Unicom Shanghai Branch，Shanghai 200050，China）

摘　要：
业务视角安全模型评估法是以业务使用流程为主线，将业务实现的全过程串接起来，形成一个端到端的，体现业务使用和网络实现的全景模型，以便全面呈现业务实际使用中的安全状态，并以是否影响业务安全来评估业务安全性的一种科学方法。有助于解决传统方式在挖掘网络隐患中存在的盲点，提升网络安全。

关键词：
业务视角；网络隐患；安全模型
doi：10.12045/j.issn.1007-3043.2024.05.014
文章编号：1007-3043（2024）05-0083-05
中图分类号：TN915
文献标识码：A
开放科学（资源服务）标识码（OSID）：

Abstract：
The security model evaluation method of business perspective is a scientific method that takes the business usage process as the main thread，connects the entire process of business implementation，and forms an end-to-end panoramic model that reflects business usage and network in order to comprehensively present the security status in actual business use，and evaluates business security based on whether it affects business security，which helps to solve the blind spots in traditional methods of mining network vulnerabilities and improves network security.

Keywords：
Business perspective；Network hidden trouble；Security model

引用格式：丁峰. 业务视角安全模型评估法[J]. 邮电设计技术，2024（5）：83-87.

1 概述

传统网络隐患排查方式由各专业从自身专业角度出发，各自领域看似安全的网络结构，却隐藏着不易被发现的盲区。这些盲区往往是在专业与专业结合点、环节与环节结合点、设备硬件与运行机制结合点，以及那些不被关注到的“小设备”。例如，一组在网络结构上相互备份冗余的2台路由设备，每台设备都配置有主备供电模块，具备相当安全等级，但被安装在同一机架并使用一路电源，1个空气开关就成为安全冗余机制的瓶颈。另一案例如图1所示，一组标准的口子型交叉互联网络拓扑结构，由于横联承担

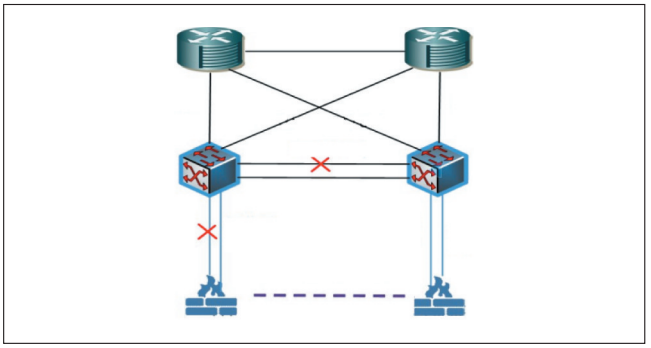

图1　故障示例拓扑

VRRP保护机制信息交互功能，当横联链路中断后，引发了VRRP机制的双主异常，最终导致所承载的业务受损。通过以上2个案例不难看出，在一些结合环节，容易出现盲区，而这些盲区隐患很难通过传统方式排

收稿日期：2024-04-16

查出来。

2 业务视角安全模型评估法定义

业务视角安全模型评估法是以业务实现路径为牵引，打破各专业壁垒，整合业务实现过程的全要素，拼接构建业务实现全景模型，并基于此模型进行安全评估与提升的方法。如图2所示，横向表示所评估业务从起点到终点的全过程，每一要素代表与业务实现相关联的独立环节，每个要素纵向展开则表示该要素所拥有独立的冗余数量。业务实现过程全要素包含了直接物理连接关系、设备内部器件连接关系、硬件与软件控制机制的连接关系（例如数据配置控制机制等）、非同维度的连接关系（例如跨弱电与强电等）、非直接接触的连接关系（例如物理空间等）。业务实现过程要素覆盖的完整性，决定了安全评估模型的基础。要素纵向冗余的独立性，决定了安全评估模型的合理性。一张完整全面的业务视角安全评估模型构建完成后，业务安全状态将清晰地展现出来，要素纵向宽度厚的（冗余数量多）安全性越高，反则安全水平低，特别是只有一层时，这会是该业务的单点安全瓶颈。如图2所示，业务视角安全模型评估法可以非常直观地识别出业务安全瓶颈，能够对业务安全性有个全面准确的评估，从方式机制上扫除了传统隐患排查方式的盲点。

3 业务视角安全模型评估法实施步骤

业务视角安全模型评估法的实施过程包括确定业务流程、编制网络拓扑、梳理现场设备资料、编制业务视角的网络拓扑、基于业务网络拓扑的安全瓶颈分析、整改措施制定6个步骤。

3.1 确定业务流程

确定业务流程重点完成2个任务。一是明确所要进行安全评估分析的业务对象；二是构建业务从起点到终点的实现全过程。这一步骤体现业务视角独特理念，也是贯穿业务视角安全模型评估法的主线。业务视角安全模型评估法对业务的定义为：一个具象的、有明确边界定义的对象。例如，一条用户传输专线。从A城用户接入点，依次通过接入网络、汇聚承载网络、核心转送网络、长途传送系统、B城的长途传送系统、核心转送网络、汇聚承载网络、接入网络，落地用户B城接入点。在这此场景下，可以依据安全评估需求确定业务对象和边界（见表1）。

表1 业务对象和边界

评估业务对象	起点	终点
用户从A点到B点专线安全评估	A点用户设备接入端口	B点用户设备接入端口
A城至B城的长途传送通路安全评估	A城长途传送设备接入端口	A城长途传送设备接入端口
接入点至核心系统传输通路安全评估	接入设备接入端口	核心传送设备接入端口

不同的业务对象定义将对后续业务安全全景图的构建，乃至安全评估和整治引发不同的结论。在初次使用业务视角安全模型评估法时，会遇到评估业务对象定义的困惑，没有明确的业务评估对象，其边界无从入手，或者陷入模糊不清的困扰中。业务视角安全模型评估法则提供了具体的方法来解决这一问题。以图3为例，本实例定义的评估业务对象是一条从A局房OTN设备端口为起始边界，依次经过OTN设备、

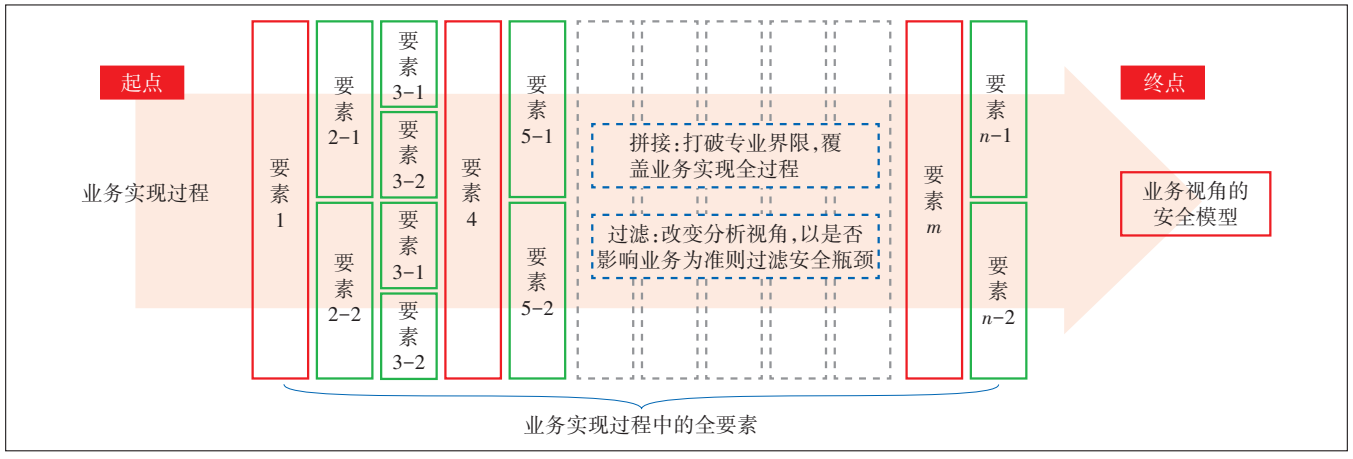

图2 业务视角安全模型评估法示意

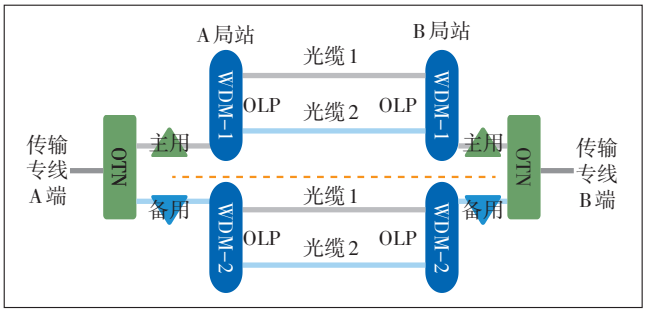

图3　业务流程

WDM设备、落地至B机房OTN设备端口的传输专线业务。评估的目标是这条传输业务的安全性。

3.2 编制网络拓扑

编制网络拓扑的重点任务是编制和汇总与评估业务对象相关的各个专业的网络拓扑。在业务视角的安全模型评估中，网络拓扑是非常重要的组成部分。业务安全的核心本质是确保网络拓扑的健壮性。业务视角安全模型评估法是转换视角，从评估对象业务的角度，将与之相关的各类网络拓扑进行拼接，从而审视评估业务的全面安全性。因此，这个环节编制的质量将直接决定了整个评估工作的有效性。以上述案例为例，需要编制的网络拓扑包括OTN网络拓扑、WDM网络拓扑、光缆管道拓扑、电气系统图、暖通系统图等主要核心网络拓扑。

3.3 梳理网元设备

梳理网元设备的重点任务是依据各个专业网络拓扑全量梳理与业务实现过程相关的所有相关要素。一是根据业务流程图，将编制的各个专业网络拓扑上的设备作为梳理的对象；二是现场查勘，将与网络拓扑所列设备有任何形式连接关系的设备纳入梳理对象。连接形式包括直接物理连接关系、硬件与软件控制机制的连接关系、非同维度的连接关系、非直接接触的连接关系等；三是将每个设备依据业务实现的功能进行拆解，形成相对独立的要素；四是将相关设备要素与业务实现的关系梳理明确。

3.4 编制业务视角网络拓扑图

依据前3个步骤所形成的信息，编制业务视角的网络拓扑图。这个步骤是业务视角安全模型评估法的核心环节，也最能体现业务视角的特征。业务网络拓扑有别于业务流程图和网络拓扑图，是以业务实现过程为主线，将其实现过程涉及的所有网元设备拼接而成的串行网络拓扑。通俗讲，就是用业务流程作为筛子，将所有涉及的各专业网元硬件、运行机制进行过滤，形成一个反映业务实现过程的网络拓扑。由于它既有业务流程，又有网络拓扑的概念，将其定义为业务网络拓扑。绘制方式如下。

a）以业务实现过程相关性为基础，用横向串接的方式将多维度的连接关系表征出来。业务实现过程中的每一个环节用1个（或多个纵向平行的）矩形表示；每一个环节具有不可替代特性，一旦不可用即业务受到影响；每个环节之间的连接关系包含直接物理连接关系、设备内部器件连接关系、硬件与软件控制机制的连接关系（例如数据配置控制机制等）、非同维度的连接关系（例如跨弱电与强电等）、非直接接触的连接关系（例如物理空间等）等5类连接关系。

b）以冗余系统的隔离有效性为标准，用纵向并联的方式将系统冗余关系表征出来。每个环节系统冗余的组建采用纵向平行并联矩形表示；每个矩形方块具有独立特性，它的不可用不影响业务；纵向平行并联矩形数量表征了该环节系统冗余能力；纵轴宽度越宽代表冗余度越大，越窄则反映出这可能是影响业务安全的瓶颈点，特别是只有唯一通路时，即存在单点安全瓶颈。我们时常会被表面的冗余现象所迷惑，这些假冗余或者有条件的冗余背后往往是安全盲点。因此在编制业务视角网络拓扑图时，对于每个并列冗余的系统功能须严格确认其独立性，即该系统的冗余组建在完全失效的情况下，其他冗余系统是否能全面承接，而不会导致业务的中断。

如图4所示，将一条从A局房至B机房传输专线业务实现过程进行了业务视角网络拓扑的编制。它包含OTN/WDM系统、设备自身、供配电系统、纤芯、光缆、管道等与业务直接或间接相关的因素，展示了该业务实现过程的全景图。

3.5 基于业务网络拓扑的安全瓶颈分析

依据业务网络拓扑进行业务安全评估重点完成2个任务，一是对业务对象进行安全状态的评估，识别安全瓶颈；二是通过分析安全瓶颈原因对编制业务视角网络拓扑图进行确认和纠正。业务视角的网络拓扑纵轴宽度越宽代表冗余度越大，越窄则可能是业务安全的瓶颈点。具体实施这个步骤时，可从2个方面着手，一是验证多系统冗余有效性；二是定位单点瓶颈的原因。

a）接入端的单点瓶颈。业务接入端往往存在单点瓶颈，时常会被忽视或回避。不同业务有各自不同的特征，通过业务视角网络拓扑图能清晰呈现出来。

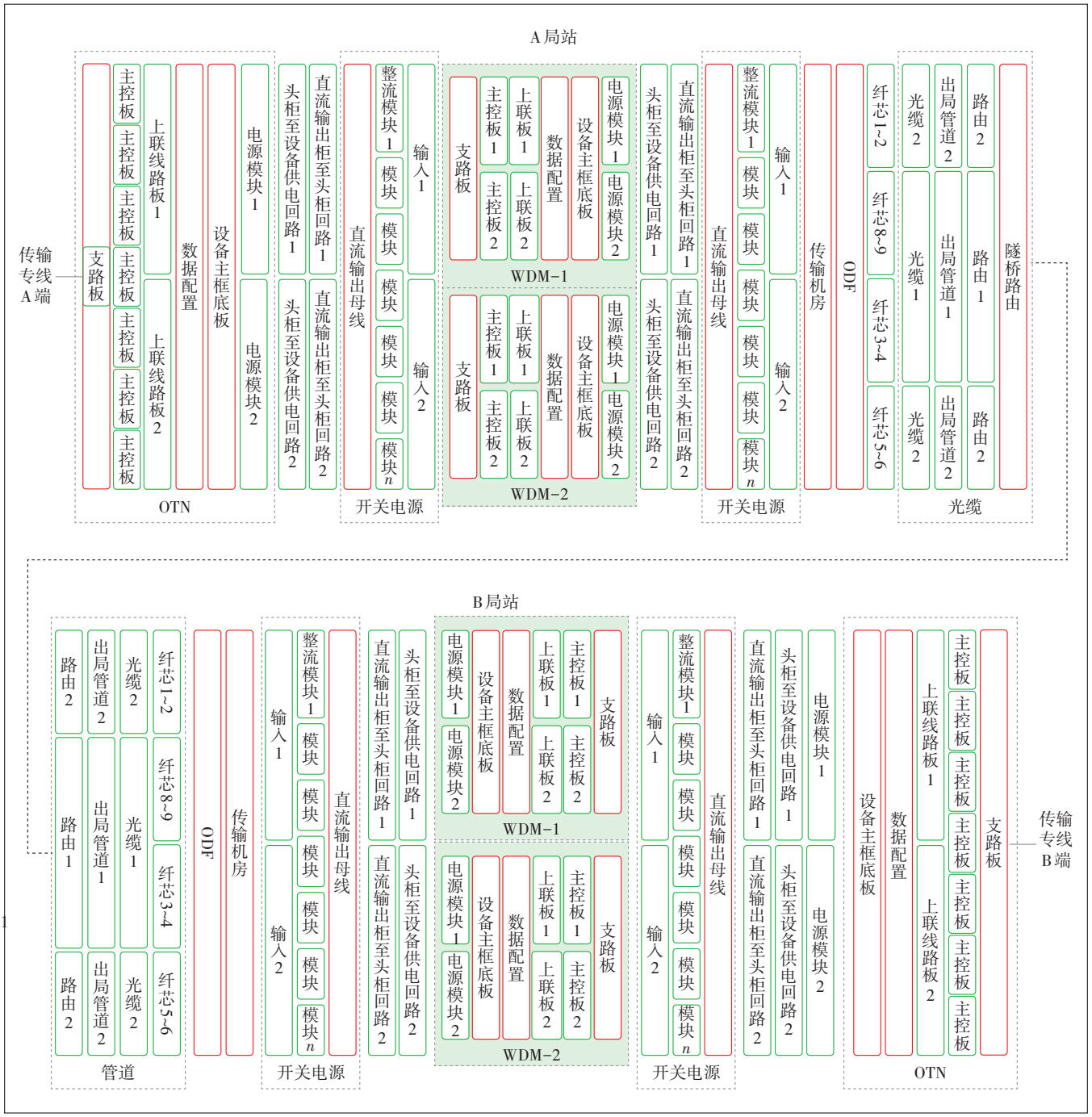

图4 业务视角网络拓扑图实例

b）OTN设备单点瓶颈。由于设备采用多主控板、双上联、双电源模块等冗余措施，安全瓶颈传统排查方式往往会被忽略，但通过业务视角安全模型评估法的环节拆解和冗余独立性分析手段，能过滤出单点瓶颈。例如OTN设备底框及数据配置是不可回避的单点问题。

c）直流输出单母线。设备配置了双电源模块、双分路供电回路，但最终终结在同一个直流母线，无法实现电气隔离。

d）WDM设备供电瓶颈。由于采用了2个平面结构，规避了类似OTN设备单板接入、单主框、数据配置的单点问题。这里也引出了“一个好的系统结构，远比一台好的设备更重要”的概念。系统结构的冗余能力能够解决设备层级无法解决的安全瓶颈问题。

WDM双平面网络结构是一个典型的正面实例，但它的配电结构则是一个反面实例。从图4可以清楚地看到，由于这2台设备接在同一个直流输出母线上，形成了新单点安全瓶颈。突破专业限制的业务视角网络拓扑就能清晰地展示这一安全瓶颈。通过进一步挖掘，发现这2台设备又同在一个传输机房，物理空间层面又产生了新的交叉点。

e）局内线路安全瓶颈。由于采用了2套系统，每套系统又采用了双上联，此环节的业务安全达到了前所未有的高度，只要4个通路没有全部中断，就能确保业务安全，但是4路光纤汇集一个ODF，产生了又一个单点瓶颈。

f）光缆同路由。2套系统4路上联，使用了2条不同的光缆，2条光缆大部分路由实现分离，但在有些路段形成了同路由的单点瓶颈。以上安全瓶颈点在业务视角安全模型评估法所构建的业务网路拓扑上被清晰识别展示出来，这正是业务视角安全模型评估法想要达到的目标。

3.6 整改提升措施制定

在实施该步骤时，应关注以下几个方面。

a）综合多个业务来确定最终安全措施。通信系统不只承载某一类业务，应将相关的业务安全评估进行整合，从而得出整体方案。

b）适配场景应对单设备瓶颈问题。针对安全要求高的核心场景，可采用双平面双活冗余模式，从网络架构上解决单设备瓶颈问题。针对业务接入末梢或冗余经济效益低的场景，可采用承载总量管控的分布式模式，即控制设备承载的业务总量，从而降低故障影响面，也是一种提升业务安全性的理念。

c）安全评估不只是加法，也可以做减法。看清楚业务实现的全过程和全环节，就能对业务安全有个正确的评价，不仅仅只是安全瓶颈，也可能有简化网络的潜力。对于业务网络拓扑所展示出来纵向冗余过多的环节，就是可以考虑网络简化的点。

d）引入直流系统双母线模式。-48 V直流系统是通信设备长期使用的供电系统，有着安全性高、绝缘要求低、设备损耗小、并接容易等诸多优势，也正是利用这样的优势，大量使用的并接方式，包括通信用电设备电源模块内部也将2路输入电源进行直接电气连接。这种方式在带来用电设备冗余的同时，也带来电气隔离不彻底的问题。由于用电设备侧形成的回路，供电侧就不得不采用统一的供电源。这也就无法避免单一直流输出母线的供电模式。随着IT类设备的出现，200~400 V交流供电模式进入通信领域。由于交流电的特征，无法实现简单的并接，所以均采用电气隔离模式，形成了双总线的冗余模式。笔者认为可以将双总线模式引入至-48 V电源系统领域，以大幅提升安全等级，但需要产业链的协同。通信设备生产方面，把电源模块的电气隔离作为行业生产标准。随着设备模块化的发展，技术上已经不是难题，目前还缺少行业强制标准。通信运营企业，应改变目前习惯的规划、建设、运维标准，从而适配这一变化，确保安全使用。

e）机房线路及ODF架的安全性应纳入安全考量范畴。局外的光缆路由安全性常被关注，局内线路安全容易被忽视。要规范这一环节，需要从机房设计、建设阶段入手。目前局内走线通道的设计，还是停留在可通达和三线分离的层面上，并没有对局内走线冗余安全性进行规划。从技术上讲，可以基于冗余考虑走线通道路由规划，提升局内路由安全性。

4 结束语

业务视角安全模型评估法突破了传统方式的专业壁垒，填补了视角盲点，从业务本质安全角度出发，构建业务安全的全景图，业务视角的网络拓扑是其核心。方法本身及其实施步骤有明确定义和具体方式，通过实例验证了其科学性和可操作性，是一种有效评估业务安全性的方法手段，对于提升网络的安全性有积极意义。若进一步向网络规划和建设环节前移，将会带来更为可观的成效。

参考文献：

[1] 李晖，狄文远. 自智网络隐患主动识别研究[J]. 电信工程技术与标准化，2023，36(8)：59-64.

[2] 张蕊，黄剑波，王如玥，等. 基于大数据的网络隐患分析系统研究与应用[J]. 数字通信世界，2024(2)：114-116.

[3] 王盼盼. 计算机网络安全隐患分析及其防范措施的探讨[J]. 计算机光盘软件与应用，2013(1)：2.

作者简介：

丁峰，工程师，学士，主要从事通信网络建设运营工作。