ICS 35.240.01
CCS L78

T/CSAC

团　　体　　标　　准

T/CSAC 022—2025

工业控制协议健壮性测试方法

Robustness Testing Method for Industrial Control Protocols

2025-07-18 发布　　2025-09-18 实施

中国网络空间安全协会　　发 布

目　　次

前　　言 II
1 范围 1
2 规范性引用文件 1
3 术语和定义 1
4 缩略语 1
5 概述 2
5.1 测试对象 2
5.2 测试要求 2
5.3 测试环境 2
6 测试项 2
6.1 报文错误注入测试 2
6.1.1 单字段变异 2
6.1.2 字段组合变异 3
6.2 报文结构变异测试 3
6.3 上下文异常测试 4
6.4 风暴测试 4
7 异常监测 4
7.1 网络服务监测 4
7.2 控制功能监测 4
8 测试方法 5
8.1 报文错误注入测试 5
8.2 报文结构变异测试 6
8.3 上下文异常测试 6
8.4 风暴测试 7
附　　录 A 8
参考文献 13

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中国网络空间安全协会提出。

本文件由中国网络空间安全协会归口。

本文件起草单位：国家计算机网络应急技术处理协调中心、西北工业大学、昆仑数智科技有限责任公司、北京信联数安科技有限公司、清华大学、武汉理工大学、华东师范大学、中国科学院软件研究所、中国网络安全审查认证和市场监管大数据中心、中国人民解放军陆军工程大学、沈阳东软系统集成工程有限公司。

本文件主要起草人：张晓明、金增旺、彭广明、姜宇、徐倩华、秦玉龙、吴涛、向剑文、苏亭、蔡彦、王峰、胡超、孙海英、蔡倩楠、贾彦生、张嘉玮、杨黎斌、赵艳阳、杜鹏、赵波、江倩、薛晓亮、景鑫、罗文杰、丁宗康、沈天翔、彭和平。

工业控制协议健壮性测试方法

1 范围

本文件给出了工业控制协议健壮性的测试方法、测试项和异常监测方法。

本文件适用于工业控制设备或工控上位机所采用的工业控制协议的通信健壮性测试,可用于指导检测机构、产品供应商等开展相关测试活动，也可用于指导相关测试工具的研发。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中,注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 25069-2022 信息安全技术 术语

3 术语和定义

GB/T 25069-2022界定的以及下列术语和定义适用于本文件。

3.1

工控上位机 industrial control host

在工业控制环境中,管理、控制工业控制设备的主机。

注：通常运行通用的操作系统，如 Windows,Unix/Linux等。

[来源:GB/T 37962-2019，3.2]

3.2

工业控制设备 industrial control device

对工业生产过程及装置进行检测与控制的设备。

[来源:GB/T 37962-2019，3.3]

3.3

工业控制协议 industrial control protocol

工业控制系统中，上位机与控制设备之间以及控制设备与控制设备之间的通信报文规约。通常包括模拟量和数字量的读写控制。

[来源:GB/T 37933-2019，3.1]

3.4

健壮性 robustness

描述网络关键设备或部件在无效数据输入或者在高强度输入等环境下,其各项功能可保持正确运行的程度。

[来源:GB 40050—2021，3.5]

4 缩略语

下列缩略语适用于本文件。

TLV：TLV编码（Type Length Value）

5 概述

工业控制协议健壮性测试主要用于验证工业控制设备或工控上位机在采用工业控制协议进行通信时，针对异常输入或高强度输入下的正确性和稳定性。

5.1 测试对象

工业控制协议健壮性测试对象为工业控制设备或工控上位机上实现的工业控制协议，如Modbus/TCP、Ethernet/IP、IEC 60870-5-104等。

5.2 测试要求

工业控制协议健壮性测试应覆盖相关协议规约中约定的所有报文类型和协议状态机，应对每种报文类型进行错误注入测试、结构变异测试和风暴测试，对每种协议状态进行上下文异常测试。

5.3 测试环境

工业控制协议健壮性测试环境通常由测试设备和测试对象组成，测试设备用于向测试对象发送异常报文或网络风暴，并实时监测测试对象运行状态。测试设备应尽量与测试对象直接相连，以避免中间网络设备造成的干扰。

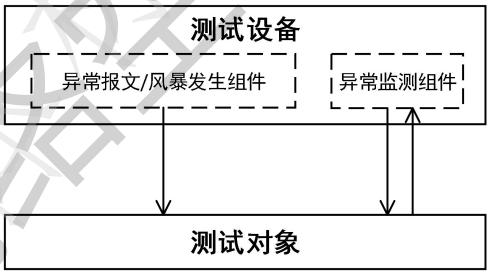

图 1 工控协议通信健壮性测试示意图

6 测试项

工业控制协议健壮性测试包括报文错误注入测试、报文结构变异测试、上下文异常测试和风暴测试。典型工业控制协议报文结构示例见附录A。

6.1 报文错误注入测试

针对协议规约的每种报文类型，构造或捕获该类型报文的典型通信样本，对通信样本中各字段进行错误注入，即对各字段值进行变异，生成测试报文并发送给测试对象，考察测试对象处理此种异常报文的健壮性。

6.1.1 单字段变异

基于通信样本报文，依次对报文各个字段值进行变异，每次只变异一个字段，直至遍历该类型报文所有字段，考察测试对象处理单字段异常报文的能力。根据报文字段长度是否变化可将字段分为定长字段和不定长字段。

6.1.1.1 定长字段变异

定长字段通常包括协议标识字段、报文长度字段、功能码/服务字段、序列号字段、校验和字段、数字签名字段等，字段的值类型包括有符号整型、无符号整型、字符串类型等。定长字段变异应满足如下要求：

a) 当定长字段为N位有符号整型数值时，变异值应覆盖两侧端点值：$-2^{(N-1)}$、$-2^{(N-1)}+1$、$+2^{(N-1)}-1$、$+2^{(N-1)}-2$和主要中间值：-2、-1、0、+1。可结合协议规约，将该字段的一个或多个典型非法值作为变异值引入。可自动生成一个或多个随机值作为变异值引入。

b) 当定长字段为N位无符号整型数值时，变异值应覆盖两侧端点值：0、1、$2^{N}-2$、$2^{N}-1$，典型中间值：$2^{(N-1)}-2$、$2^{(N-1)}-1$、$2^{(N-1)}$、$2^{(N-1)}+1$。可结合协议规约，将该字段的一个或多个典型非法值作为变异值引入。可自动生成一个或多个随机值作为变异值引入。

c) 当定长字段为N字节字符串时，应根据字符串长度进行变异，变异值应包括特殊字符（如“reboot”、“shutdown”等系统命令字符，“\r”、“\n”换行符，“%s”、“%n”等格式化符）、空字符串和违反编码规则的字符串（如非法的字符编码或字符集）。

d) 对于重要功能字段，如功能码、子功能码、服务字段等，变异值可覆盖该字段的所有合法值和典型非法值。在N较小情况下，变异值可遍历字段所有可能数值。

e) 在对定长字段进行变异时，应确保报文中其他非变异字段值的正确性，如校验和字段、数字签名字段等。

6.1.1.2 不定长字段变异

不定长字段通常包括用户名、文件名等自限制长度的字符串字段、TLV结构等。不定长字段变异应满足如下要求：

a) 当不定长字段为自限制长度的字符串类型时，变异值应包括含特殊字符（如“reboot”、“shutdown”等系统命令字符，“\r”、“\n”换行符，“%s”、“%n”等格式化符）、空字符串、超长字符串和违反编码规则的字符串（如非法的字符编码或字符集）。

b) 当不定长字段为TLV结构时，应结合Type字段取值首先确定Value字段值类型，根据Value字段值类型对其变异。Length字段未变异时取值应与变异值长度保持一致。

c) 当不定长字段值超过单报文最大长度时，可根据协议规约对报文进行分片。

d) 在对不定长字段进行变异时，应确保报文中其他非变异字段值的正确性，如校验和字段、数字签名字段、长度字段等。

6.1.2 字段组合变异

基于通信样本报文，选取两个或多个报文字段同时进行变异，考察测试对象处理此种异常报文的能力。组合变异的字段可选取重要功能字段或语义相关的字段（如：对于Modbus/TCP协议，同时对协议标识和长度字段进行变异、同时对功能码和子功能字段进行变异）。

组合变异选取的字段数量不宜过大，可通过限制字段变异值数量、限制变异组合数量，将变异报文数量控制在可接受范围内。

6.2 报文结构变异测试

针对协议规约的每种报文类型，根据报文结构将报文划分为标识部分、控制部分、数据部分、选项部分等，对划定部分进行变异，包括重复、删除、截断、位置变换等操作，即报文结构变异，生成测试报文，考察测试对象处理此种结构异常报文的能力。在结构变异中，应保证非变异部分字段值处于有效范围。

6.3 上下文异常测试

根据协议规约，发送前置报文，使测试对象协议状态机处于指定状态，在该状态下向测试对象发送非预期协议报文，考察测试对象处理此种上下文异常的能力。非预期报文可从当前协议状态下不应收到的报文类型中选取。测试应覆盖协议状态机所有状态。

6.4 风暴测试

根据协议规约，选取一种报文类型，构造或捕获该协议状态的典型通信样本，以线速或接近测试对象最大处理能力的速率发送样本报文，并持续120秒以上，考察测试对象在风暴停止后，其网络服务能否在测试对象约定时间内恢复正常。如测试对象具备控制功能，可同时考察测试对象在风暴测试过程中其控制输出有无异常。风暴测试应覆盖协议规约中的所有报文类型。

7 异常监测

异常监测包括网络服务监测和控制功能监测，主要用于考察测试对象在报文错误注入测试、报文结构变异测试、上下文异常测试或风暴测试中，其网络状态或控制功能是否出现异常。

7.1 网络服务监测

网络服务监测要求如下：

a) 在报文错误注入测试、报文结构变异测试和上下文异常测试过程中，应对测试对象的网络状态进行实时监测，考察测试对象的网络状态在测试过程中是否出现异常。

b) 对于风暴测试，应在风暴停止后监测测试对象的网络状态，考察测试对象的网络状态能否在合理时间内恢复正常。

c) 可从不同层面对测试对象网络状态进行监测，如通过ICMP协议监测测试对象的IP可达性、通过SNMP协议监测测试对象的系统状态、通过工控协议端口状态监测测试对象工控服务的可用性、通过工控协议状态监测报文或控制报文监测测试对象的协议功能有无异常。

d) 应为测试对象设定合理的网络状态监测周期，监测周期过短会降低测试效率、过长会导致异常状态被遗漏。对于测试对象系统或服务进程重启速度较快、出现异常难以发现的情况，可采用基于TCP长连接的协议功能监测方式进行异常监测。

7.2 控制功能监测

对于具备控制功能的测试对象，可通过专用信号采集模块对测试对象的控制输出波形进行实时采集与分析，可根据测试对象厂商声明的控制输出抖动最大容差和置信度（一般不低于95%），考察测试过程中控制输出是否出现异常抖动。

注1：抖动是指信号事件被检测到的时间与基于参考信号的预期时间之间的差异。在需要精确同步的工业场合，异常抖动会导致控制过程中的不确定性。

注2：置信度以百分比表示，表示预期有该比例的抖动测量值小于最大容差。例如抖动最大容差为50ms和置信度为95%，则意味着预计95%的抖动测量值将小于50ms。

8 测试方法

8.1 报文错误注入测试

针对协议规约的每种报文类型，构造或捕获该类型报文的典型通信样本，对通信样本中各字段进行错误注入，生成测试报文并发送给测试对象，考察测试对象处理此种异常报文的能力。

8.1.1 单字段变异测试

a) 预置条件：
   1) 对测试对象进行配置，使其工控协议相关业务功能处于有效状态。
   2) 如测试对象支持控制功能，配置其控制输出模块周期性输出指定波形，用于控制功能监测。
b) 检测步骤：
   1) 启动异常监测组件，对测试对象的网络服务状态或控制输出进行实时监测。
   2) 根据协议规约，选定一种协议报文类型，构造或捕获该类型报文的通信样本，样本内容应与测试对象配置参数相匹配。
   3) 向测试对象发送样本报文，分析测试对象反馈报文，验证样本报文能否被正确处理。如样本报文类型需要测试对象处于特定协议状态，则应先发送前置报文使其到达测试所需状态，再发送样本报文。
   4) 如样本报文可被正确处理，则基于样本报文，选定一个报文字段，根据字段类型对该字段值进行变异；同时重新计算报文长度、校验和、签名等字段值，以保证非变异字段的有效性；生成测试报文，发送给测试对象，监测测试对象有无异常。如样本报文需要测试对象处于特定协议状态，则应先发送前置报文使其到达测试所需状态，再发送测试报文。
   5) 重复本节步骤4，依次遍历该字段需覆盖的全部变异值。
   6) 重复本节步骤4-5，依次对样本报文所有字段进行变异。
   7) 重复本节步骤2-6，依次对协议规约中约定的所有报文类型进行单字段变异测试。
   8) 可根据测试对象性能调整测试报文发送速率和异常监测周期，以提升测试效率。
c) 预期结果：
   在测试过程中，异常监测组件未检测到测试对象的网络状态异常（如 IP 不可达、TCP/UDP 工控协议服务端口不可达、协议功能异常等）或控制输出异常。
d) 判定原则：
   测试结果应与预期结果相符。

8.1.2 字段组合变异测试

a) 预置条件：
   1) 对测试对象进行配置，使其工控协议相关业务功能处于有效状态。
   2) 如测试对象支持控制功能，配置其控制输出模块周期性输出指定波形，用于控制功能监测。
b) 检测步骤：
   1) 启动异常监测组件，对测试对象的网络服务状态或控制输出进行实时监测。
   2) 根据协议规约，选定一种协议报文类型，构造或捕获该类型报文的通信样本，样本内容应与测试对象配置参数相匹配。
   3) 向测试对象发送样本报文，分析测试对象反馈报文，验证样本报文能否被正确处理。如样本报文类型需要测试对象处于特定协议状态，则应先发送前置报文使其到达测试所需状态，再发送样本报文。

4）如样本报文可被正确处理，则基于样本报文，从中选取两个或多个字段组合进行变异；同时重新计算报文长度、校验和、签名等字段值，以保证非变异字段的有效性；生成测试报文，发送给测试对象，监测测试对象有无异常。如样本报文类型需要测试对象处于特定协议状态，则应先发送前置报文使其到达测试所需状态，再发送测试报文。

5）重复本节步骤4，依次遍历选定字段的所有变异值组合。

6）重复本节步骤4-5，依次选取重要功能字段或语义相关字段进行组合变异。

7）重复本节步骤2-6，依次对协议规约中约定的所有报文类型进行组合变异。

8）可根据测试对象性能调整测试报文发送速率和异常监测周期，以提升测试效率。

c）预期结果：

在测试过程中，异常监测组件未检测到测试对象的网络状态异常（如 IP 不可达、TCP/UDP 工控协议服务端口不可达、协议功能异常等）或控制输出异常。

d）判定原则：

测试结果应与预期结果相符。

8.2 报文结构变异测试

a）预置条件：

1）对测试对象进行配置，使其工控协议相关业务功能处于有效状态。

2）如测试对象支持控制功能，配置其控制输出模块周期性输出指定波形，用于控制功能监测。

b）检测步骤：

1）启动异常监测组件，对测试对象的网络服务状态或控制输出进行实时监测。

2）根据协议规约，选定一种协议报文类型，构造或捕获该类型报文的通信样本，样本内容应与测试对象配置参数相匹配。

3）向测试对象发送样本报文，分析测试对象反馈报文，验证样本报文能否被正确处理。如样本报文类型需要测试对象处于特定协议状态，则应先发送前置报文使其到达测试所需状态，再发送样本报文。

4）如样本报文可被正确处理，则基于样本报文，从中选取一个报文结构对其进行变异；同时重新计算报文长度、校验和、签名等字段值，以保证非变异字段值的有效性；生成测试报文，发送给测试对象，监测测试对象有无异常。如样本报文类型需要测试对象处于特定协议状态，则应先发送前置报文使其到达测试所需状态，再发送测试报文。

5）重复本节步骤4，依次对选定报文结构进行各种变异，包括复制、删除、截断、位置变换等。

6）重复本节步骤4-5，依次遍历样本报文的所有结构。

7）重复本节步骤2-6，依次对协议规约中约定的所有报文类型进行结构变异测试。

8）可根据测试对象性能调整测试报文发送速率和异常监测周期，以提升测试效率。

c）预期结果：

在测试过程中，异常监测组件未检测到测试对象的网络状态异常（如 IP 不可达、TCP/UDP 工控协议服务端口不可达、协议功能异常等）或控制输出异常。

d）判定原则：

测试结果应与预期结果相符。

8.3 上下文异常测试

a）预置条件：

1）对测试对象进行配置，使其工控协议相关业务功能处于有效状态。

2）如测试对象支持控制功能，配置其控制输出模块周期性输出指定波形，用于控制功能监测。

b）检测步骤：

1）启动异常监测组件，对测试对象的网络服务状态或控制输出进行实时监测。

2）根据协议规约，选定一种协议状态，发送前置报文使测试对象到达测试所需协议状态。

3）向测试对象发送该协议状态下的非预期报文，非预期报文应为格式和内容均正确且与测试对象配置参数相匹配的报文，监测测试对象有无异常。

4）重复本节步骤3，至少覆盖3种非预期报文。非预期报文类型应尽量为当前状态语义相关报文。

5）重复本节步骤2-4，依次对协议规约中约定的所有协议状态进行上下文异常测试。

c）预期结果：

在测试过程中，异常监测组件未检测到测试对象的网络状态异常（如 IP 不可达、TCP/UDP 工控协议服务端口不可达、协议功能异常等）或控制输出异常。

d）判定原则：

测试结果应与预期结果相符。

8.4 风暴测试

a）预置条件：

1）对测试对象进行配置，使其工控协议相关业务功能处于有效状态。

2）如测试对象支持控制功能，配置其控制输出模块周期性输出指定波形，用于控制功能监测。

b）检测步骤：

1）启动异常监测组件，对测试对象的网络服务状态或控制输出进行实时监测。

2）根据协议规约，选定一种协议报文类型，构造或捕获该类型报文的通信样本，样本内容应与测试对象配置参数相匹配。

3）向测试对象发送样本报文，分析测试对象反馈报文，验证样本报文能否被正确处理。如样本报文类型需要测试对象处于特定协议状态，则应先发送前置报文使其到达测试所需状态，再发送样本报文。

4）如样本报文可被正确处理，则以线速或接近测试对象最大处理能力的速率持续发送样本报文，发送时间不少于120秒，监测测试对象有无异常。

5）重复本节步骤2-4，依次对协议规约中约定的所有报文类型进行风暴测试。

c）预期结果：

在测试过程中，异常监测组件未检测到测试对象的控制输出异常；在风暴停止后，测试对象的网络状态能够在测试对象约定的时间内恢复正常。

d）判定原则：

测试结果应与预期结果相符。

附 录 A
（资料性）
典型报文结构示例

A.1 概述

本附录包含工业控制协议健壮性测试中常见的报文字段、报文结构以及协议状态示例。需要强调的是，这些仅是示例，详细报文信息，需参考相关协议规约。

A.2 定长字段示例

表 A.1 展示了Modbus/TCP协议中的功能码字段示例，其中包含了事务处理标识符字段、协议标识符、长度字段、功能码等定长字段。

表 A.1 功能码字段示例

字段分类	描述	大小（byte）	示例	数值范围
MBAP 报文头	事务处理标识符 Hi	2	0x1501	0~65535
	事务处理标识符 Lo			
	协议标识符	2	0x0000	0
	长度	2	0x0006	0~65535
	单元标识符	1	0xFF	0~255
Modbus 请求	功能码	1	0x03	0~255
	起始地址	2	0x0004	0~65535
	寄存器数量	2	0x0001	0~65535

A.3 变长字段示例

图A.1展示了IEC61850 MMS协议典型报文，该协议使用ASN.1(抽象语法记法一)中的BER（基本编码规则），表 A.2 为报文TLV结构解析表。

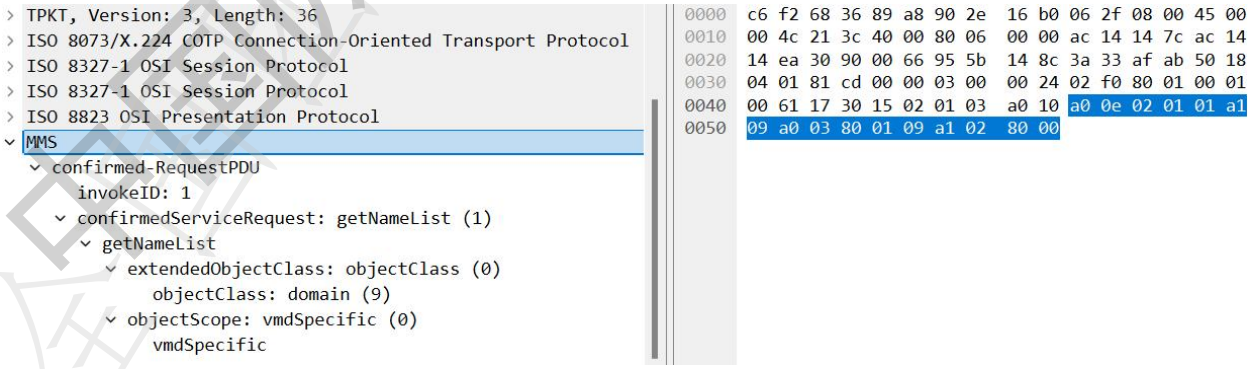

图 A.1 IEC61850 MMS示例报文

表 A.2 MMS示例报文解析

类别		报文		说明
		十六进制	二进制	
TLV1				
类型（Type）	高 2 位	a0	10100000	2：上下文特定类
	第 3 位			1：构造类型
	低 5 位			0:confirmed-RequestPDU
长度（Length）		0e	-	长度为 14 字节
值（Value）		02 01 01 a1 09 a0 03 80 01 09 a1 02 80 00	-	包含嵌套结构，TLV2、TLV3、TLV4、TLV5、TLV6、TLV7
TLV2				
类型（Type）	高 2 位	02	00000010	0：通用类
	第 3 位			0：基本类型
	低 5 位			2：整数
长度（Length）		01	-	长度为 1 字节
值（Value）		01	-	整数值 1，invokeID
TLV3				
类型（Type）	高 2 位	a1	10100001	2：上下文特定类
	第 3 位			1：构造类型
	低 5 位			1：getNameList
长度（Length）		09	-	长度为 9 字节
值（Value）		a0 03 80 01 09 a1 02 80 00	-	包含嵌套结构,TLV4、TLV5、TLV6、TLV7
TLV4				
类型（Type）	高 2 位	a0	10100000	2：上下文特定类
	第 3 位			1：构造类型
	低 5 位			0：objectClass
长度（Length）		03	-	长度为 3 字节
值（Value）		80 01 09	-	包含嵌套结构，TLV5
TLV5				
类型（Type）	高 2 位	80	10000000	2：上下文特定类
	第 3 位			0：基本类型
	低 5 位			0：nammedVariable
长度（Length）		01	-	长度为 1 字节
值（Value）		09	-	值为 9，表示 domain

表 A.2（续）

类别		报文		说明
		十六进制	二进制	
TLV6				
类型（Type）	高 2 位	a1	10100001	2：上下文特定类
	第 3 位			1：构造类型
	低 5 位			1：objectScope
长度（Length）		02	-	长度为 2 字节
值（Value）		80 00	-	包含嵌套结构，TLV7
TLV7				
类型（Type）	高 2 位	80	10000000	2：上下文特定类
	第 3 位			0：基本类型
	低 5 位			0：vmdSpecific
长度（Length）		00	-	长度为 0 字节

A.4 报文结构划分示例

表A.3展示了Modbus/TCP协议读取文件记录功能（0x14）典型报文，将该报文划分为报文头、功能以及参数三个结构。

表 A.3 结构划分示例

报文结构	字段描述		大小（byte）	示例	数值范围
报文头	事务处理标识符 Hi		2	0x1501	0~65535
	事务处理标识符 Lo				
	协议标识符		2	0x0000	固定值
	长度		2	0x0006	0~65535
	单元标识符		1	0xFF	0~255
功能	功能码		1	0x14	0~255
	字节计数		1	7*N	0~255
参数	子请求 1	引用类型	1	0x01	0~255
		文件号	2	0x0006	0~65535
		记录号	2	0x0001	0~65535
		记录长度	2	0x0064	0~65535
	子请求 2	引用类型	1	0x0001	0~255
		文件号	2	0x06	0~65535
		记录号	2	0x0001	0~65535
		记录长度	2	0x0064	0~65535
	…	…	…	…	…
	子请求 N	引用类型	1	0x0001	0~255
		文件号	2	0x06	0~65535
		记录号	2	0x0001	0~65535
		记录长度	2	0x0064	0~65535

A.5 协议状态示例

图A.2展示了IEC61850 MMS协议getNameList服务简要交互状态示意图。

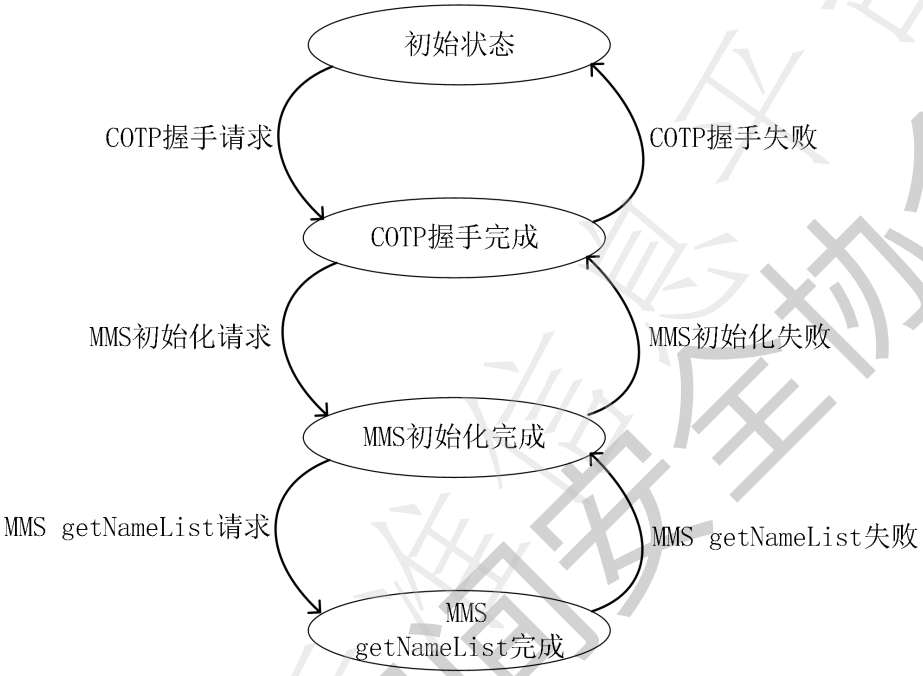

图 A.2 IEC61850 MMS示例报文getNameList服务简要交互状态

参考文献

[1] GB/T 28456-2012《IPsec协议应用测试规范》
[2] GB 40050-2021《网络关键设备安全通用要求》
[3] EDSA-310-2.2 《ISA Security Compliance Institute – Embedded Device Security Assurance –Requirements for embedded device robustness testing》