

网络靶场 试验任务导调总体要求

General Requirements for Task Directing

（征求意见稿）

2023-03-15

XXXX – XX – XX 发布 XXXX – XX – XX 实施

中国网络安全空间安全协会 发布

目 次

目 次..... I

前 言..... II

网络靶场 试验任务导调总体要求..... 1

1 范围..... 1

2 规范性引用文件..... 1

3 术语和定义..... 1

 3.1 导调方（黄方） yellow team..... 1

 3.2 平台管理方（白方） white team..... 1

 3.3 评估方（绿方） green team..... 1

 3.4 攻击方（红方） red team..... 1

 3.5 防御方（蓝方） blue team..... 2

4 概述..... 2

5 试验任务导调流程..... 2

 5.1 试验任务一般流程..... 2

 5.2 试验任务调度流程要求..... 3

6 试验任务导调中的五方状态描述与流转要求..... 4

 6.1 黄方状态描述与流转要求..... 4

 6.2 白方状态描述与流转要求..... 5

 6.3 绿方状态描述与流转要求..... 6

 6.4 红蓝方状态描述与流转要求..... 7

7 试验任务导调中的通信要求..... 8

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并归口。

本文件起草单位：鹏城实验室、哈尔滨工业大学（深圳）、广州大学网络空间先进技术研究院、中国信息通信研究院、北京永信至诚科技股份有限公司、四川亿览态势科技有限公司、软极网络技术（北京）有限公司、湖南星汉数智科技有限公司、电子科技大学、北京理工大学、中汽创智科技有限公司、广东为辰信息科技有限公司、重庆长安汽车股份有限公司、中国电信股份有限公司广东研究院、中国联合网络通信有限公司、中国移动通信集团有限公司、南方电网科学研究院有限责任公司、中国电子信息产业集团有限公司第六研究所、北京天融信网络安全技术有限公司、博智安全科技股份有限公司。

本文件主要起草人：贾焰、胡宁、邱欣逸、李树栋、曲博、顾钊铨、韩伟红、安伦、蔡晶晶、陈俊、李润恒、陶莎、黄九鸣、谢玮、孟楠、罗蕾、危胜军、杨彦召、薛信钊、汪向阳、王帅、金华敏、邱勤、陈璐、李雪莹、王龔、匡晓云、杨祎巍、傅涛、郑轶、徐天妮、陶冶、赵焕宇、燕玮、王绍杰、张凯、李炜。

网络靶场 试验任务导调总体要求

1 范围

本文件对网络靶场试验任务导调进行了总体要求,包括试验任务的一般流程,以及为完成试验任务,黄方、白方、红方、蓝方和绿方等主要五方角色的状态流转情况。

本文件适用于指导网络靶场的设计、开发、建设和应用。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件。凡是不注日期引用文件,其最新版本(包括所有的修改单)适用于本文件。

2019-0981T-YD 网络安全空间仿真 术语

3 术语和定义

在 2019-0981T-YD 中界定的术语和定义适用于本文件。

3.1

导调方(黄方) **yellow team**

通常被称作黄方,是事态的导调方。在事态计划准备阶段,黄方负责确定事态需求、制定事态计划,并且对整个事态过程进行控制与管理,对事态数据进行查询分析、回放、归档等。

[来源: 2019-0981T-YD, 3.248]

3.2

平台管理方(白方) **white team**

通常被称作白方,是事态的平台管理方。为整个事态过程提供技术保障。白方需要根据黄方的事态计划,完成整个仿真环境的搭建,包括虚拟网络生成、实物网络配置、虚实互联以及网络服务生成等内容。此外在事态实施过程中,白方需要进行攻防情报的收集,包括数据采集与处理、状态监控、态势显示以及数据存储等内容。在试验结束阶段,白方还负责事态资源的净化释放。

[来源: 2019-0981T-YD, 3.249]

3.3

评估方(绿方) **green team**

通常被称作绿方,是事态的评估方。绿方负责对事态运行阶段平台管理方(白方)收集到的各类事态数据与攻防情报进行详尽分析,对攻防效果进行评估,并出具相关评估报告。

[来源: 2019-0981T-YD, 3.252]

3.4

攻击方(红方) **red team**

通常被称作红方，是事态的攻击方。红方需要在事态实施前制定攻击计划，根据计划完成攻击技术研制与部署，在事态实施过程中，按照计划对防御方实施网络攻击行为。

[来源：2019-0981T-YD，3.250]

3.5

防御方（蓝方） blue team

通常被称作蓝方，是事态的防御方。蓝方需要在事态实施前制定防御计划，根据计划完成防御技术的部署，在事态实施过程中，对来自攻击方的网络攻击实施防御行为，或利用/攻击对手系统以保护网络阵地。

[来源：2019-0981T-YD，3.251]

4 概述

网络靶场基于一组软硬件资源仿真一个目标网络，提供五方系统，供黄方、白方、红方、蓝方和绿方等主要五方角色协同使用。网络靶场作为支撑网络攻防演练、网络安全技术测评、网络安全人才培养和网络新技术验证重大基础设置，应包括以下五大能力：

- a) 黄方系统应具备导调指挥功能，完成试验的统一管理。
- b) 白方系统应具备目标网络仿真与互联接入功能，提供试验环境。
- c) 绿方系统应具备攻击检测与态势评估功能，完成试验过程的攻击检测和态势评估。
- d) 红方系统应具备攻击工具管理及组装部署功能，为试验人员提供攻击工具。
- e) 蓝方系统应具备防御工具管理及协同运行功能，为试验人员提供防御工具。

本文件对网络靶场的导调指挥进行描述和要求，包括试验任务一般流程、试验导调总要求、试验各阶段描述、五方状态流转等。

5 试验任务导调流程

5.1 试验任务一般流程

试验任务的生命周期如图 1 所示，从创建到归档一般经历试验准备阶段、试验运行阶段以及试验结束阶段。

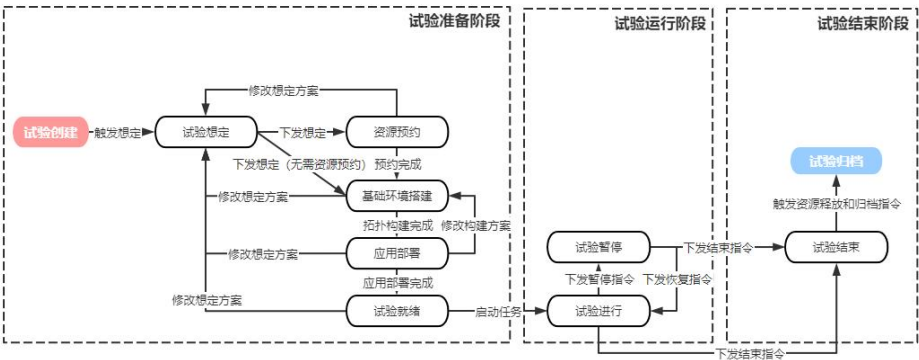


图 1 试验生命周期示意图

在试验的整个生命周期中五方系统相互协作，共同保证试验的顺利进行。各阶段任务如下：

- a) 试验准备阶段：主要完成试验想定以及环境部署等；
- b) 试验运行阶段：主要是对试验状况的监控以及对试验的控制；
- c) 试验完成阶段：主要完成资源的释放以及对试验数据的归档。

5.2 试验任务调度流程要求

5.2.1 试验任务调度要求总览

导调指挥功能由黄方系统实现，提供试验创建、试验查看、试验想定、试验下发、试验部署进度监控、试验过程控制和监视、试验归档等功能，总体要求如下：

- a) 应提供面向多靶场协同工作的试验演练的统一管理，应提供多靶场协同的试验演练并发调度；
- b) 应提供靶场能力、靶标及场景资源、攻防工具资源等的统一描述；
- c) 应提供面向多靶场协同的各类资源注册和管理；
- d) 应提供面向多靶场的任务全生命周期的实时监控能力；
- e) 应支持多靶场协同的想定方案快速生成、校验和资源预约；
- f) 应支持多靶场协同试验的统一控制：支持分布式统一资源管理和试验控制，支持对分靶场的资源进行统一管理，支持接收来自联邦靶场的统一控制指令，并开展分布式试验任务，能够向其他分靶场等下发试验控制指令。

5.2.2 试验准备阶段

试验准备阶段的主要工作是，对试验的实施方案以及所需的资源进行想定，并根据想定方案进行环境部署。具体要求如下：

- a) 试验创建：黄方人员根据试验场景选择对应的配置模板创建一个新的试验；
- b) 试验想定：黄方人员填写试验的基本信息、并完成资源、人员、任务等一系列配置，在想定结束之后，将想定信息下发给白、红蓝、绿等其他方；
- c) 资源预约：白方接收到黄方的想定方案后，应根据实际情况确定是否需要进行资源预约；当需要进行资源预约时，白方应根据想定方案确定所需要的资源类型以及数量，并对资源所有方下发预约请求，完成资源的锁定，避免出现后续部署不成功的问题；
- d) 基础环境搭建：当白方确定无需资源预约或资源预约已完成，进入到基础环境搭建。在此过程中，白方将根据想定的方案完成基础环境的搭建，保证整个环境是可供其他方访问和部署应用的，同时在搭建过程中，白方应根据试验需要定时汇报搭建进度并暴露可能存在的风险；
- e) 应用部署：白方构建完基础环境后，会将构建的基础环境信息传递给红蓝、绿方。红蓝、绿、白应在基础环境下，根据试验想定的要求进行应用部署，并定时向黄方汇报部署进度。部署的应用包括但不限于绿方的采集探针，红蓝方的攻防工具，并最终由部署方验证试验所需应用和工具被有效部署；
- f) 试验就绪：当各方都准备就绪，并向黄方反馈准备完成后，试验进入到就绪状态。

在试验准备阶段，黄方根据各方定时上报的信息，持续监视各方的部署情况，当部署情况无法满足需求或临时出现需求变更时，黄方都能触发想定修改，使试验重新进入到试验想定状态。

5.2.3 试验运行阶段

当试验准备就绪且黄方无需再修改方案后，黄方可根据试验计划触发试验启动，至此试验正式进入试验运行阶段。

a) 试验进行：试验启动后，进入到试验运行状态，黄方宜持续监控各方状态，包括但不限于，白方提供的试验环境信息，绿方提供的数据采集和分析情况，红蓝方提供的选手或环境的监控情况等；此状态下，白方始终监控和维护试验环境情况，绿方实时采集实验数据并进行分析，红蓝方系统为试验人员提供操作环境并监控其行为。

b) 试验暂停：根据试验需要和各方反馈情况，黄方可对试验执行暂停操作，此时各方系统需确保选手不能再执行操作，同时根据试验的需要，各方可配合完成各项操作，包括但不限于：

- 1) 调整部署环境，如修复故障机器、新增监控探针、增删资源和靶标等操作；

- 2) 试验流程修改，如根据试验情况，调整试验运行的步骤与流程；
- 3) 方案优化，如根据试验情况解释判分规则或新增提示等操作。

如果调整成功，黄方可通过恢复指令使试验重新进入试验进行阶段；如果调整失败，黄方可根据试验情况选择放弃调整继续进行试验或者直接结束试验；在试验运行阶段，暂停与恢复可在试验运行阶段多次执行，直到试验结束。

5.2.4 试验结束阶段

- a) 试验结束阶段主要是完成资源的释放以及数据的归档。
- b) 试验结束：黄方下发结束指令，白方系统需保证试验人员无法访问试验环境；红蓝方系统需关闭试验人员的操作权限；绿方系统需停止采集和分析工作等；
- c) 试验归档：将试验数据进行落盘归档，方便后续对试验进行回放和查看；同时各方应根据需要释放占用的资源；并在释放完成后通知黄方，以便其更新试验状态。

6 试验任务导调中的五方状态描述与流转要求

6.1 黄方状态描述与流转要求

黄方进行试验时的状态流转以及状态转换的触发条件如图 2 所示。

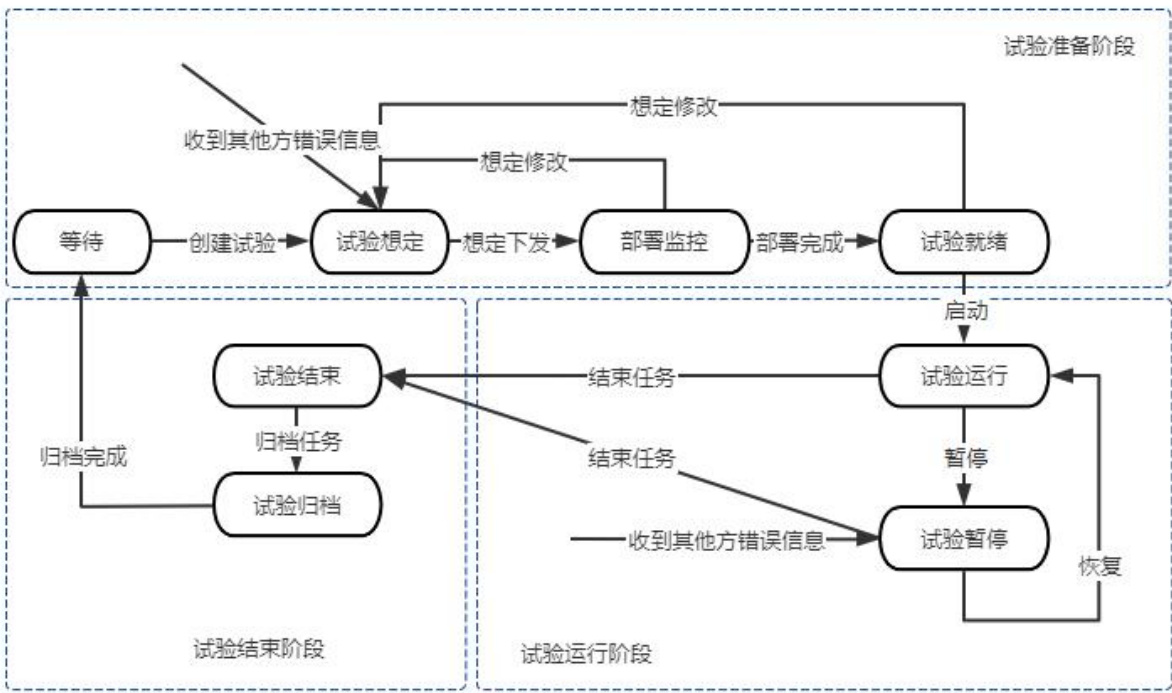


图 2 黄方状态流转

黄方状态流转的描述和要求如下：

- a) 等待：无试验需求时，黄方处于等待状态；
- b) 试验想定：通过选择试验类型来创建试验后，黄方状态由等待切换到试验想定状态；在试验想定状态下，黄方人员根据试验类型获得想定模板，然后根据模板填写试验的基本信息、人员配置、资源配置以及试验配置等数据；在试验启动之前，黄方应能在任何状态下，主动触发重回试验想定状态，从而完成想定方案的修改，以应对突发状况；

c) 部署监控：想定方案确定后，黄方将想定方案下发给红蓝、绿、白等其他方，即进入部署进度监控状态。在此状态下，黄方宜实时监控各方对想定方案的准备情况，如果执行过程中出现各方无法独立解决的错误，黄方回退到试验想定，对已有想定方案进行修改，保证试验环境顺利准备；

d) 试验就绪：黄方确定各方的部署完成后，从部署监控进入到试验就绪状态，等待试验启动；

e) 试验运行：黄方根据试验规划触发试验启动，从而黄方进入试验运行状态；在试验运行阶段，黄方将持续从白、绿、红、蓝四方获取状态信息，实时监视试验的运行情况，并根据需要为运维人员提示可能存在的风险。

f) 试验暂停：在试验运行状态下，黄方可根据试验需要，对试验下发暂停指令，黄方即进入试验暂停状态。当黄方处于试验暂停状态时，可以根据试验情况指导其他方完成试验环境调整、优化试验流程等工作，并实时监控其他方的执行情况，如果各方执行完成，黄方可通过恢复试验重新进入到试验运行状态，如果执行失败，黄方可根据试验情况选择放弃调整，重新回到试验运行状态，或执行结束命令，使状态切换到试验结束；在试验运行阶段，黄方应能在接收到其他方的错误信息时，自动进入到试验暂停状态，只有当问题解决之后，才可通过恢复试验重新进入到试验运行状态；

g) 试验结束：黄方下发结束命令后，状态从试验运行切换到试验结束状态；

h) 试验归档：针对结束的试验，黄方可下发归档指令，完成试验数据的落盘，进入到试验归档状态。在此状态下，黄方会监控白、绿、红、蓝四方资源回收和数据落盘情况，当黄方确认四方完成归档指定后，黄方会更新试验状态，并再次进入等待状态，等待新试验的创建。

6.2 白方状态描述与流转要求

白方进行试验时的状态流转以及状态转换的触发条件如图 3 所示。

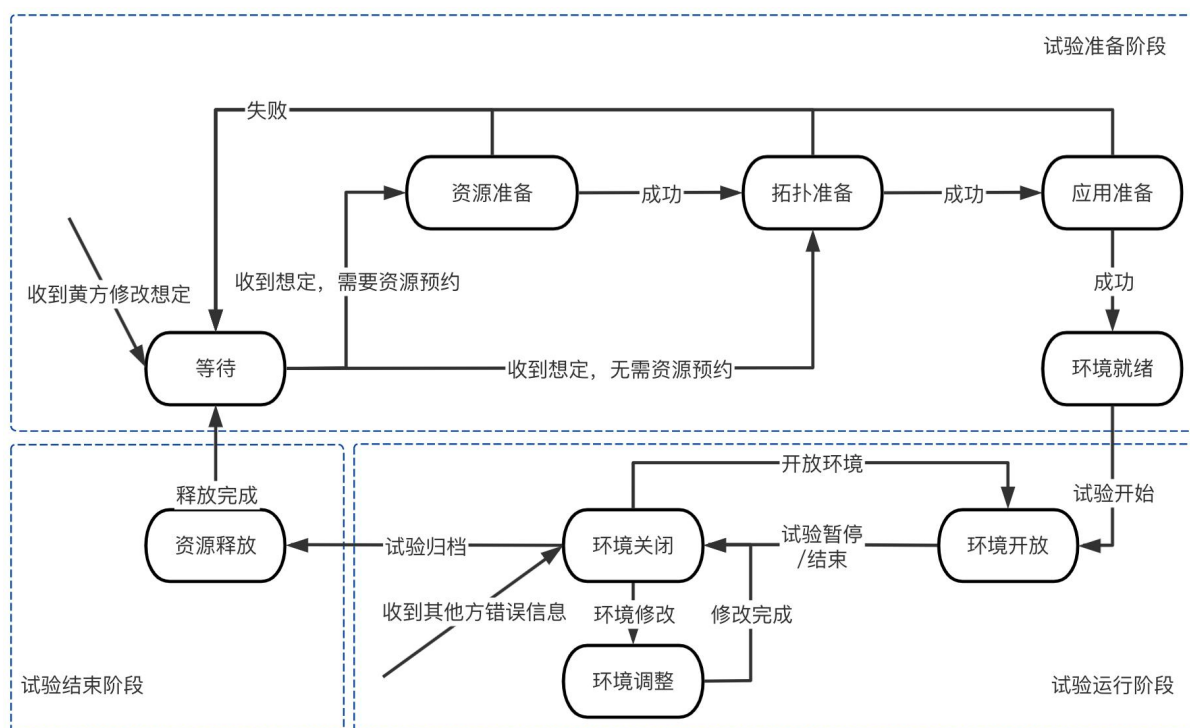


图 3 白方状态流转

白方状态流转的描述和要求如下：

a) 等待：未接收到想定方案、黄方主动触发方案修改以及出现无法自行解决的错误时，白方应进入等待状态；

b) 资源准备：接收到黄方下发的想定方案后，白方应对想定进行分析，确定需要进行资源预约则

进入资源准备状态；此状态下，白方应根据想定方案所需要的资源类型和数量等情况，与资源所有方协商预约请求资源，完成资源的锁定；

c) 拓扑准备：在成功完成资源准备或收到想定方案且无需资源预约时，白方应根据想定方案完成试验基础环境的构建，确保其他方可根据想定方案进行试验环境准备；

d) 应用准备：基础环境构建成功后，白方进入应用准备状态；此状态下，白方应在基础环境的上，进一步完成其他部署和配置；

e) 环境就绪：全部准备完成后，白方应从应用准备状态进入环境就绪状态；

f) 环境开放：试验开始后，白方应进入环境开放状态；在此状态下，白方环境为试验人员开放，允许其进行访问与操作；同时白方会定时向黄方汇报白方环境的状态信息，使其能及时掌握环境状态，为后续决策提供依据。

g) 环境关闭：白方接收到暂停指令或接收到错误报告后，状态从环境开放迁移到环境关闭，此状态下不允许试验人员在实验环境上进行任务操作与访问；

h) 环境调整：根据试验的需要，白方可在环境关闭状态进入到环境调整状态，以对环境进行调整，在环境调整之前，白方会先对环境进行备份，若调整成功，当调整结束后将自动切换到环境关闭状态，等待试验重启；若调整失败，且收到黄方继续比赛的指令，白方将会恢复备份环境，并切换到环境关闭状态，等待试验重启；若调整失败，且收到黄方结束指令后，白方将直接切换到环境关闭状态；

i) 资源释放：接收到试验归档指令后，白方应进入资源释放状态，并在资源释放完成后向黄方发送释放完成的信号，在得到黄方确认后，重新进入等待状态。

6.3 绿方状态描述与流转要求

绿方进行试验时的状态流转以及状态转换的触发条件如图 4 所示。

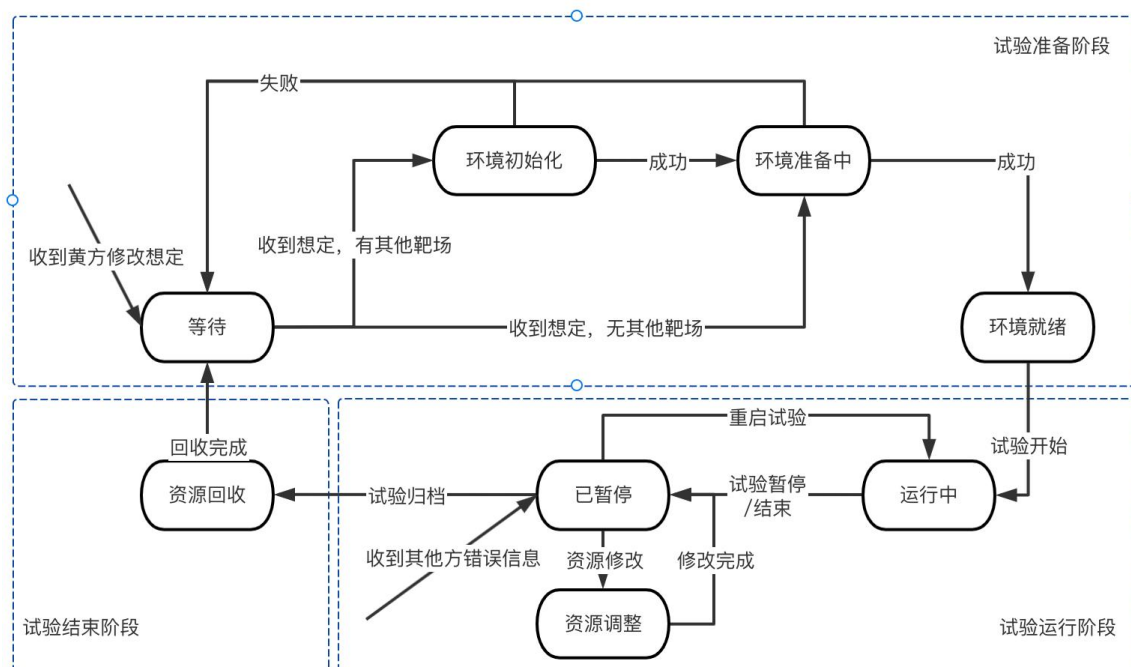


图 4 绿方状态流转

绿方状态流转的描述和要求如下：

a) 等待：未接收到想定方案、黄方主动触发方案修改以及出现无法自行解决的错误时，绿方应进入等待状态；

b) 环境初始化：接收到想定方案，并确定需与其他靶场联合试验后，绿方应进入环境初始化状态；

在此状态下，绿方需同步其他靶场的能力，以作为后续环境准备的依据；

c) 环境准备中：收到黄方想定并确定无需其他靶场协同试验，或环境初始化结束后，绿方进入环境准备状态；在此状态下，绿方根据试验需要进行资产探测、部署采集探针等试验前全部准备，并定时向黄方汇报部署进度；

d) 环境就绪：环境准备成功后，绿方向黄方发送环境准备就绪信号，在得到黄方确认后，绿方进入环境就绪状态，等待黄方下达后续指令；

e) 运行中：试验开始后，绿方进入运行中状态；在此状态下，绿方应持续进行试验数据采集和分析，并根据试验类型进行可视化展示，同时定时向黄方汇报所需信息；

f) 已暂停：当试验暂停、结束，或接收到错误报告后，绿方应进入到暂停状态，即试验运行阶段的等待状态；

g) 资源调整：绿方可按需进入资源调整状态，在资源调整之前，绿方会先对环境配置进行备份，若调整成功，当调整结束后将自动切换到已暂停状态，等待试验重启；若调整失败，且收到黄方继续比赛的指令，绿方将会恢复环境，并切换到已暂停状态，等待试验重启；若调整失败，且收到黄方结束指令后，绿方将直接切换到已暂停状态；

h) 资源回收：接收到试验归档指令后，应进入资源回收状态，完成资源的释放与回收，并在结束之后向黄方发送回收完成的信号，在得到黄方确认后，重新进入等待状态。

6.4 红蓝方状态描述与流转要求

红蓝方进行试验时的状态流转以及状态转换的触发条件如图 5 所示。

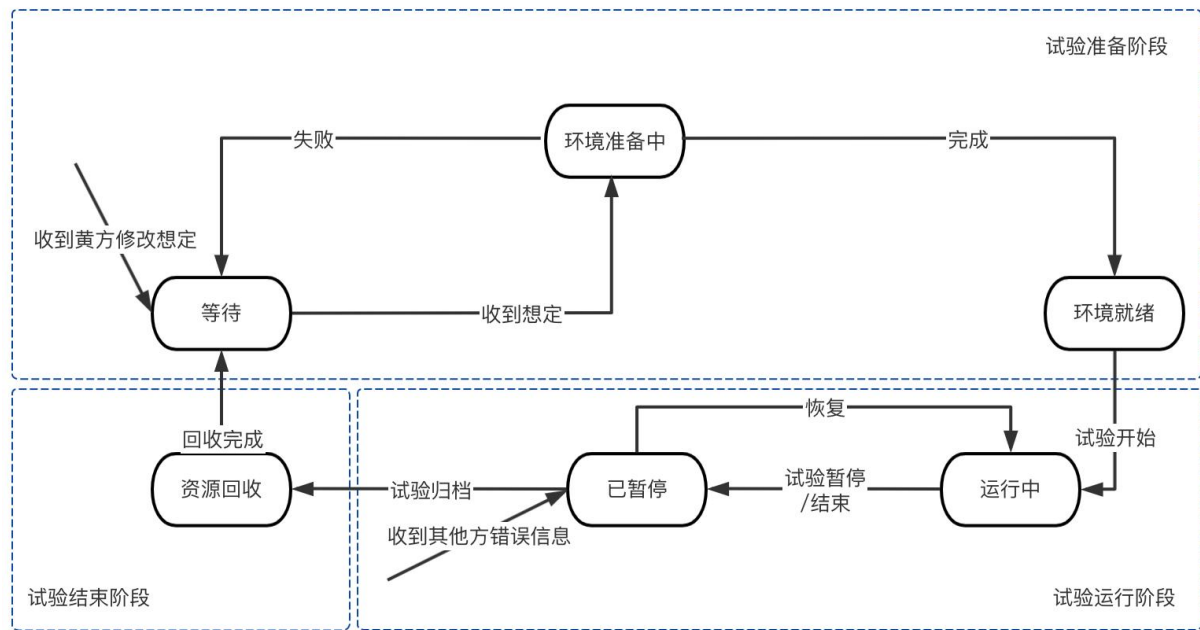


图 5 红蓝方状态流转

红蓝方状态流转的描述和要求如下：

a) 等待：未接收到想定方案、黄方主动触发方案修改以及出现无法自行解决的错误时，红蓝方系统应进入等待状态；

b) 环境准备中：接收到想定方案后，红蓝方系统应进入到试验准备状态；在此状态下，红蓝方系统需完成攻防武器的部署等环境准备工作，并根据需要准备试验人员的接入设备，同时定时向黄方汇报部署进度；；

c) 环境就绪：环境准备成功后，红蓝方向黄方发送环境准备就绪信号，在得到黄方确认后，红蓝方系统自动进入就绪状态等待黄方后续指令；

d) 运行中：试验开始后，红蓝方系统进入运行中状态；在此状态下，红蓝方系统应保证试验人员能正常、合规地进行试验，同时定时向黄方汇报所需信息；

e) 已暂停：接收到黄方下发的暂停、结束指令，或收到错误报告时，红蓝方系统进入已暂停状态；在此状态下，红蓝方系统应保证试验人员无法再进行一切与试验有关的操作；

f) 资源回收：接收到试验归档指令后，红蓝方系统应进入资源回收状态，完成资源的释放与回收，并在结束之后向黄方发送回收完成的信号，在得到黄方确认后，重新进入等待状态。

7 试验任务导调中的通信要求

g) 在试验的整个生命周期中五方系统需通过接口相互通信，在通信过程中，需满足如下要求：

a) 支持身份认证和授权：任何两方系统在进行通信时，需先对双方的身份进行认证，并赋予对应的权限，对交互双方进行访问控制。

b) 支持数据安全传输：在数据传输过程中可按需采用加密技术，保证数据传输过程的机密性；可按需采用数据完整性保护技术保证数据在传输过程中的完整性，并在检测到完整性受到破坏时采取必要的恢复措施；

c) 支持高并发数据传输：可按需使用负载均衡等技术，保证通信接口在高并发场景下依然可以稳定、高效地提供服务。

d) 支持弱网环境下的数据传输：可按需使用断点续传、数据重传等技术，保证通信接口在弱网环境下依然可以正常接收数据。

e) 通信接口定义需满足自描述性：接口的名称和参数需具有实际意义，方便不同系统间的对接与维护。