



DNC Pro 数控程序管理系统

CNC PROGRAM MANAGEMENT SYSTEM

使用说明书

文档版本 V1.0.0

深圳市彼络科技有限公司

Bivrost Technologies Company Limited

目 录

安全与注意事项

1 概述

2 应用背景与目标问题

3 系统构成

4 接入与初始配置

4.1 接入网关与机台

4.2 首次程序下发

5 操作说明

5.1 程序库与版本

5.2 审批与放行

5.3 机台分配与落地转换

5.4 程序下发

5.5 试制

5.6 滚动镜像与快照

5.7 机边修改的处置

5.8 机边操作台

5.9 系统管理与审计

6 参考资料

6.1 角色与权限

6.2 机床系统差异

6.3 REST API

6.4 日常核查

6.5 术语表

7 常见问题与故障处置

修订记录

安全与注意事项

本章为强制性内容，适用于 DNC Pro 系统的全部配置、操作与管理人员。使用本系统前应完整阅读本章。

一 提示分级

本说明书采用三级提示，含义与使用场合按表 0-1 的规定。

表 0-1 提示分级

级别	含义	忽略后果
警告	涉及人身安全、设备完好与不可逆数据损失的强制性要求	可能造成机床停机、工件报废、加工事故或程序永久丢失
注意	涉及操作正确性与数据一致性的强制性要求	可能造成操作失败、状态不一致或权限拒绝
说明	补充信息、边界条件与设计意图	不影响安全，但可能影响理解与判断效率

三级提示在正文中以提示框呈现，示例如下。

警告

警告级提示的内容为强制性要求，不得省略执行。

注意

注意级提示的内容为强制性要求，忽略将导致操作结果不符合预期。

说明

说明级提示为补充信息。

二 适用人员

本系统的操作人员应符合表 0-2 规定的资质要求。角色与权限的完整定义见 6.1。

表 0-2 适用人员与资质要求

角色	承担工作	资质要求
管理员	系统配置、账号与权限配置、令牌与外发订阅管理、审计核查	熟悉本单位信息安全制度，具备账号与权限管理经验
程序员	程序上传、版本维护、机台分配、试制下发	具备数控编程资质，熟悉目标机床的控制系统特性
审批员	版本审批与放行	具备工艺或质量审核授权
操作工	已发布版本的下发、机边操作台使用	经本系统操作培训，具备目标机床的操作资质
只读	查阅程序、传输记录与审计日志	无特殊要求

警告

本系统对机床文件系统执行删除与写入操作。未取得机床操作资质的人员不得执行下发操作，也不应被授予 `deployments.send.released` 或 `deployments.send.proveout` 权限。

三 运行安全

三.1 下发前的确认

警告

下发将删除机床上的目标文件后重新写入。执行下发前应确认目标机床未处于加工状态，且目标程序未被机床调用。对正在运行的程序执行下发可能造成加工中断或工件报废。

下发前应逐项确认：

- a) 目标机台的分配关系正确，落地文件名与路径符合该机床的命名规则（见 5.3）；
- b) 待下发版本处于「已发布」状态，或为经批准的试制版本；
- c) 机床处于待机状态，操作面板已切换至可接收外部程序的模式；
- d) 该机台无未处置的机边修改记录（见 5.7）。

三.2 试制程序的管理

警告

试制版本未经完整审批流程，不得用于批量生产。试制到期后系统不会自动撤回机床上的程序，应由责任人显式执行转正或撤回。

试制的完整规程见 5.5。对量产节拍机，应在机组级别启用禁止试制。

三.3 回滚失败的处置

下发事务在任一阶段失败时自动使用快照回滚。回滚结果为「回滚失败」时，机床上文件的实际内容不确定。

警告

回滚结果为「回滚失败」的文件处于内容未知状态。应在恢复生产前由具备机床操作资质的人员到机边核对实际程序内容，确认无误后方可继续加工，不得依据系统显示的版本号直接投产。

回滚失败的记录在设备页与机边操作台上持续显示，直至下一次成功的校验将其清除。事务阶段与回滚规则见 5.4。

三.4 机边修改

注意

本系统不会自动覆盖机床上的内容。滚动镜像捕获到的机边修改以待处置版本的形式排队，应由工程师比对差异后决定采纳或驳回。将受控版本推回机床是一次独立的显式操作。

四 数据安全

四.1 凭据保管

注意

交付时提供的管理员初始密码应在首次登录后立即经「右上角账户菜单 → 修改密码」更换，且不应在多人之间共用同一管理员账号。

a) 网关密钥与服务令牌的明文仅在创建时显示一次，应按本单位密钥管理制度保管；

b) 服务令牌应按最小权限与最小范围授予，不再使用时应及时吊销；

- c) 演示数据集中的账号与口令为公开示例值，不应用于生产环境。

四.2 审计与追溯

审计日志为只增不改的哈希链，记录每一次状态变更与每一次程序内容外流。

注意

审计日志是质量追溯的依据。不应通过直接操作数据库的方式修改或删除审计记录，此类操作将导致哈希链完整性校验失败。

四.3 备份

机床上的内容由滚动镜像持续备份并形成历史快照；本系统自身的数据按交付时约定的策略 定期备份。

警告

备份默认存放于本系统所在的服务器上，服务器整机故障时该备份同时失效。使用单位应确认备份已同步至本系统主机之外的存储。核查方法见 6.4。

关闭滚动镜像将同时放弃备份能力与机边修改检测能力。

五 使用环境

- a) 本系统按局域网内使用设计，可在完全断网条件下运行，不应直接暴露于公共网络；
- b) 本系统与彼络物联网关之间的网络应保持可达。网络中断期间下发任务将失败，机床保持原有内容不变，网关恢复后应确认机台的「最近校验」重新更新；
- c) 车间触摸屏的使用要求见 5.8.8。

六 责任边界

本系统的功能边界如下，超出边界的事项由使用单位自行负责：

- a) **不采集加工数据。** 产量、OEE、报警与刀具寿命由彼络物联网关及上层系统负责，本系统仅管理加工程序；

- b) **不代替人员决策。** 到期的试制不会被自动撤回，机床上被修改的程序不会被自动覆盖，二者均停留在界面上等待人工处置；
- c) **不校验程序正确性。** 本系统保证机床上的内容与受控版本一致，不判断该程序的工艺正确性与加工安全性；
- d) **不提供云端服务。** 全部数据存储于使用单位自有服务器。

1 概述

1.1 编写目的

本说明书规定 DNC Pro 数控程序管理系统的接入配置方法、操作方法、参考资料与故障处置措施，作为该系统的随机技术文件使用。

1.2 适用读者

本说明书适用于使用单位的系统管理员、工艺工程师、工艺主管、设备管理人员与 数控机床操作人员。各岗位对应的条款索引见 5 章导言。

1.3 文档约定

章节编号。正文按第 1 章至第 7 章编号，条款采用 章.节.条 三级编号，例如 5.4.3。「安全与注意事项」与「修订记录」为不编号的前置章与后置章。

图表编号。图与表按章编号，格式为 图 章-序号、表 章-序号，例如图 5-4、表 5-13。图题置于图下方，表题置于表上方。交叉引用采用「见图 5-4」「见表 5-13」「见 5.4.3」的形式。

提示分级。全书使用警告、注意、说明三级提示，其含义与使用场合见 安全与注意事项。

术语。全书术语以 6.5 术语表为准。同一概念只使用一种称谓，规范用词与不推荐用词的对照见表 6-17。

界面元素。界面上的按钮、菜单、字段名以「」标注，例如单击「下发」。命令、路径、请求头、权限码等以等宽字体标注，例如 `deployments.send.released`。

1.4 系统简介

DNC Pro 是运行于使用单位车间局域网内的 CNC 加工程序管理系统。它架设于一台或多台 彼络物联网网关之上，将零件、工序、程序版本与机床上 实际内容之间的对应关系，由人工记忆与共享文件夹转为可查询、可审批、可追溯的系统记录。

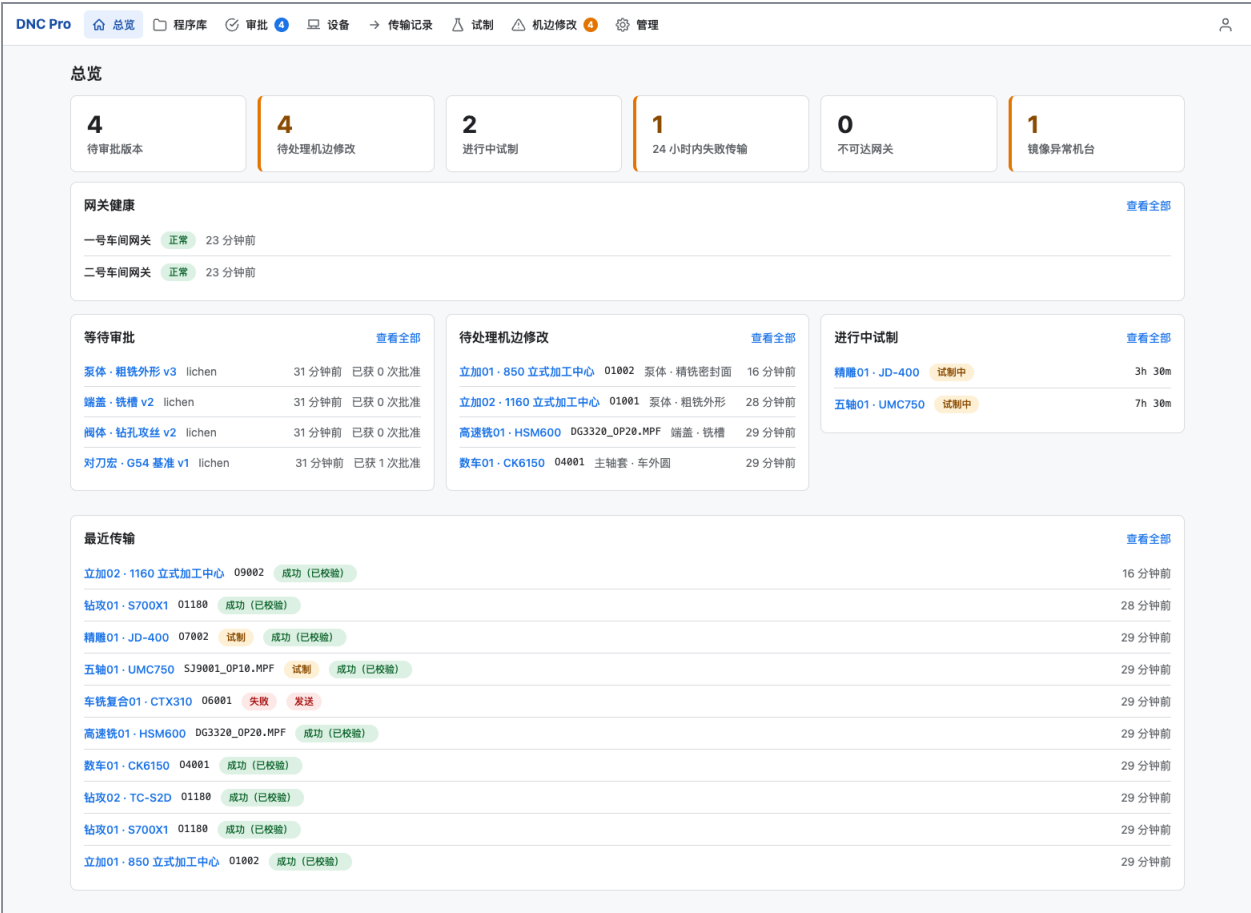


图 1-1 管理控制台总览页面

总览页集中显示当班需关注的项目：待审批版本、机边修改、进行中的试制、失败传输与网关健康状态。

1.5 功能构成

本系统的功能按表 1-1 的规定构成六条主线。

表 1-1 功能构成

功能	说明	条款
程序库与版本	程序按版本管理，经「草稿 → 待审批 → 已发布 → 废弃」流转；内容按哈希去重，任意两版可并排比对	5.1
事务式下发	预检 → 快照 → 删除 → 发送 → 回读 → 校验；任一阶段失败自动回滚快照。仅在回读内容与发送内容一致时判定为成功	5.4

功能	说明	条款
试制	显式的限时操作，全部界面带徽标； 到期后由人员决定转正或撤回，系统 不自动改动机床	5.5
滚动镜像	全天候备份每台机床上的每个文件； 机边修改被自动捕获为待处置版本， 系统不自动还原	5.6
角色与权限	五个固定角色（管理员、程序员、审 批员、操作工、只读）× 授权范围 （机组、程序库）；本地账号可完全 离网，亦可对接 OIDC 单点登录	6.1
审计	只增不改的哈希链日志，记录每一次 状态变更与每一次程序内容外流，支 持查询、CSV 导出与链完整性校验	5.9

1.6 界面构成

本系统提供两个前端，二者均为同一套 REST API 的客户端，不存在未公开接口。界面构成按表 1-2 的规定。

表 1-2 界面构成

界面	访问地址	使用人员	主要内容
管理控制台	http://<主机>:8030/	工艺、质量、设备管理人 员	程序库、审批、设备、传 输记录、试制、机边修 改、系统管理
机边操作台	http://<主机 >:8030/shopfloor/	车间工位操作人员	授权范围内的机台及其应 运行的程序



图 1-2 机边操作台的机台页面

机边操作台仅显示当前操作工授权范围内的机台，以及该机台应当运行的程序， 详见 5.8。

1.7 不适用范围

本系统不提供下列功能， 相关需求应由其他系统承担：

- a) **不采集加工数据。** 产量、OEE、报警与刀具寿命由彼络物联网关及上层系统负责， 本系统仅管理加工程序；
- b) **不代替人员决策。** 到期的试制不会被自动撤回， 机床上被修改的程序不会被自动覆盖， 二者均停留在界面上等待人工处置；
- c) **不提供云端服务。** 全套系统运行于使用单位的局域网内， 全部数据存储于使用单位 自有服务器， 可在完全断网条件下运行。

完整的责任边界见安全与注意事项。

1.8 关于本说明书中的截图

本说明书的全部截图取自一套演示数据集， 其构成为： 两台车间网关、 10 台不同控制系统的机床、 三个程序库、 六名不同角色的人员， 以及一批已执行完成的下发、 试制与机边修改记录。

截图中的零件号、 程序名与人员姓名均为示例值， 与任何实际客户无关。 演示数据集的复现方法见 4 章导言。

2 应用背景与目标问题

2.1 适用范围

本章列出以共享文件夹、U 盘与人工记忆方式管理加工程序时的六类典型失效场景， 并给出本系统的对应措施。本章用于实施前的适用性判定， 不含操作步骤。

各场景与措施的对应关系汇总见表 2-1。

表 2-1 失效场景与对应措施

场景	失效表现	本系统的措施	条款
2.2	无法确认机床上运行的是哪一版	版本由系统统一编号，滚动镜像持续核对	5.1、 5.6
2.3	传输中断留下不完整程序	事务式下发，回读校验通过方判定成功	5.4
2.4	机边改动无人知晓，下次下发被覆盖	自动捕获为待处置版本，不自动覆盖机床	5.7
2.5	试制程序遗留在机床上被当作正式程序	试制限时、带徽标，到期由人处置	5.5
2.6	控制器数据丢失导致程序无法恢复	全天候备份机床上的每一个文件	5.6
2.7	无法回答某批零件的程序、审批与下发记录	只增不改的哈希链审计日志	5.9

2.2 场景一：无法确认机床上的版本

失效表现。 程序以文件名区分版本，出现 泵体粗铣_最终版.nc、泵体粗铣_最终版2.nc、泵体粗铣_最终版_改进给.nc 等并存的文件，无法确认机床上运行的程序来源于哪一个。

本系统的措施。 程序在系统中具有唯一身份（零件号 + 工序），版本号由系统递增。每台机台上的每个受管文件记录最后一次成功下发的版本号，并由滚动镜像持续核对机床上的 实际内容是否仍为该版本。

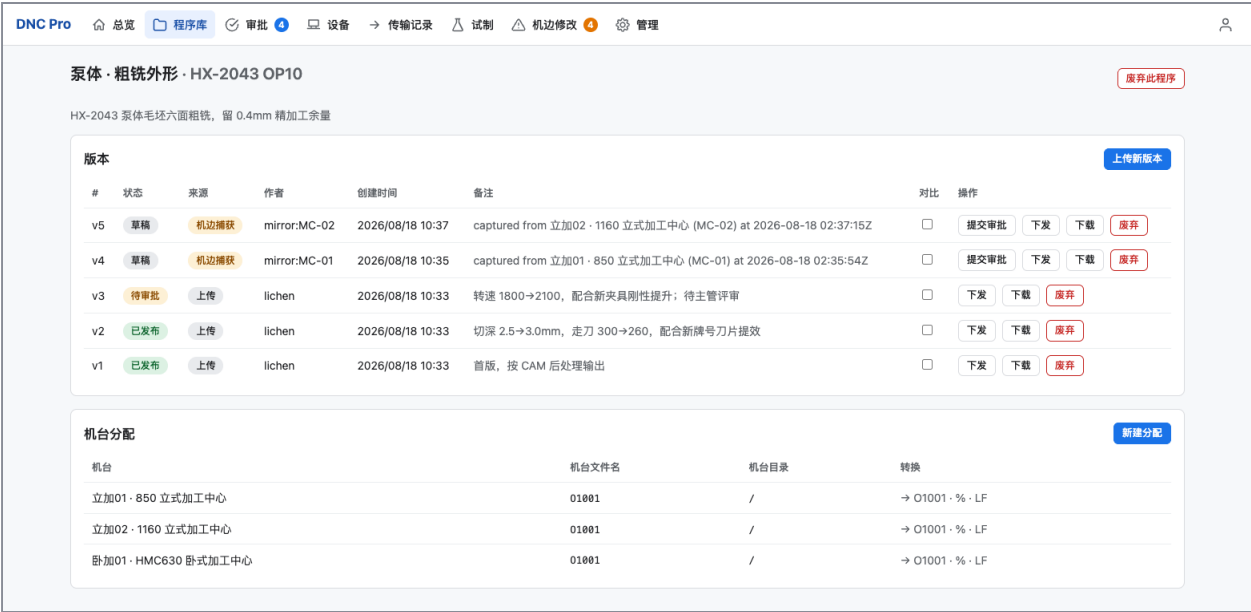


图 2-1 程序详情页面的版本历史

图 2-1 中，v1、v2 为已发布版本，v3 为待审批版本，v4 与 v5 为自机床捕获的机边修改。每一版的来源、作者与备注均有记录。

2.3 场景二：传输中断留下不完整程序

失效表现。RS-232 断线、网络抖动、机床内存不足、程序号被锁定等原因导致传输中断，机床上留下不完整的程序，而操作人员误认为已完成。

本系统的措施。每一次下发构成一个事务，执行阶段见图 2-2。

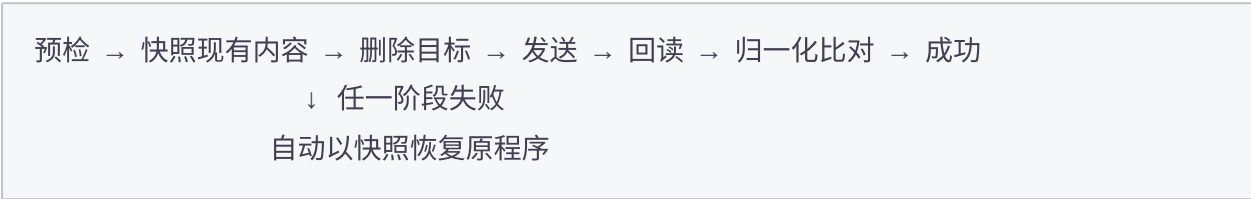


图 2-2 下发事务的阶段与失败回滚

下发结果仅在回读内容与发送内容比对一致时判定为成功。删除阶段之后的任何失败均触发快照回滚，机床不会停留在无内容或内容不完整的状态。

DNC Pro

总览

程序库

审批

设备

传输记录

试制

机边修改

管理

刷新

机台

全部机台

状态

全部状态

共 16 条, 0 进行中, 1 失败

机台	文件	状态	失败阶段	回滚	试制	排队时间	完成时间
立加02 · 1160 立式加工中心	09002	成功 (已校验)				2026/08/18 10:48:44	2026/08/18 10:48:44
钻攻01 · S700X1	01100	成功 (已校验)				2026/08/18 10:37:14	2026/08/18 10:37:14
精雕01 · JD-400	07002	成功 (已校验)			试制	2026/08/18 10:35:45	2026/08/18 10:35:45
五轴01 · UMC750	SJ9001_0P10.MPF	成功 (已校验)			试制	2026/08/18 10:35:44	2026/08/18 10:35:44
车铣复合01 · CTX310	06001	失败 send failed: Network fault.	发送	已回滚		2026/08/18 10:35:44	2026/08/18 10:35:44
高速铣01 · HSM600	DG3320_0P20.MPF	成功 (已校验)				2026/08/18 10:35:35	2026/08/18 10:35:35
数车01 · CK6150	04001	成功 (已校验)				2026/08/18 10:35:34	2026/08/18 10:35:34
钻攻02 · TC-S2D	01100	成功 (已校验)				2026/08/18 10:35:34	2026/08/18 10:35:34
钻攻01 · S700X1	01100	成功 (已校验)				2026/08/18 10:35:34	2026/08/18 10:35:34
立加01 · 850 立式加工中心	01002	成功 (已校验)				2026/08/18 10:35:33	2026/08/18 10:35:33
卧加01 · HMC630 卧式加工中心	09002	成功 (已校验)				2026/08/18 10:35:33	2026/08/18 10:35:33
立加02 · 1160 立式加工中心	09002	成功 (已校验)				2026/08/18 10:35:33	2026/08/18 10:35:33
立加01 · 850 立式加工中心	09002	成功 (已校验)				2026/08/18 10:35:33	2026/08/18 10:35:33
卧加01 · HMC630 卧式加工中心	01001	成功 (已校验)				2026/08/18 10:35:32	2026/08/18 10:35:32
立加02 · 1160 立式加工中心	01001	成功 (已校验)				2026/08/18 10:35:32	2026/08/18 10:35:32
立加01 · 850 立式加工中心	01001	成功 (已校验)				2026/08/18 10:35:32	2026/08/18 10:35:32

图 2-3 传输记录页面

图 2-3 中失败的一条明确记录失败阶段（发送）与回滚结果（已回滚），无需到机边确认。完整规则见 5.4。

2.4 场景三：机边改动无人知晓

失效表现。操作工在机床上调整加工参数。该改动通常基于现场判断且正确， 但仅存在于该台机床的存储中，工艺人员无从知晓，下一次下发即将其覆盖。

本系统的措施。滚动镜像检出受管文件内容变化时，将其捕获为待处置版本并在控制台排队， 由工程师查看差异后决定采纳或驳回。

注意

本系统不自动覆盖机床。即使决定驳回，将受控版本推回机床仍是一次需要显式勾选的操作。

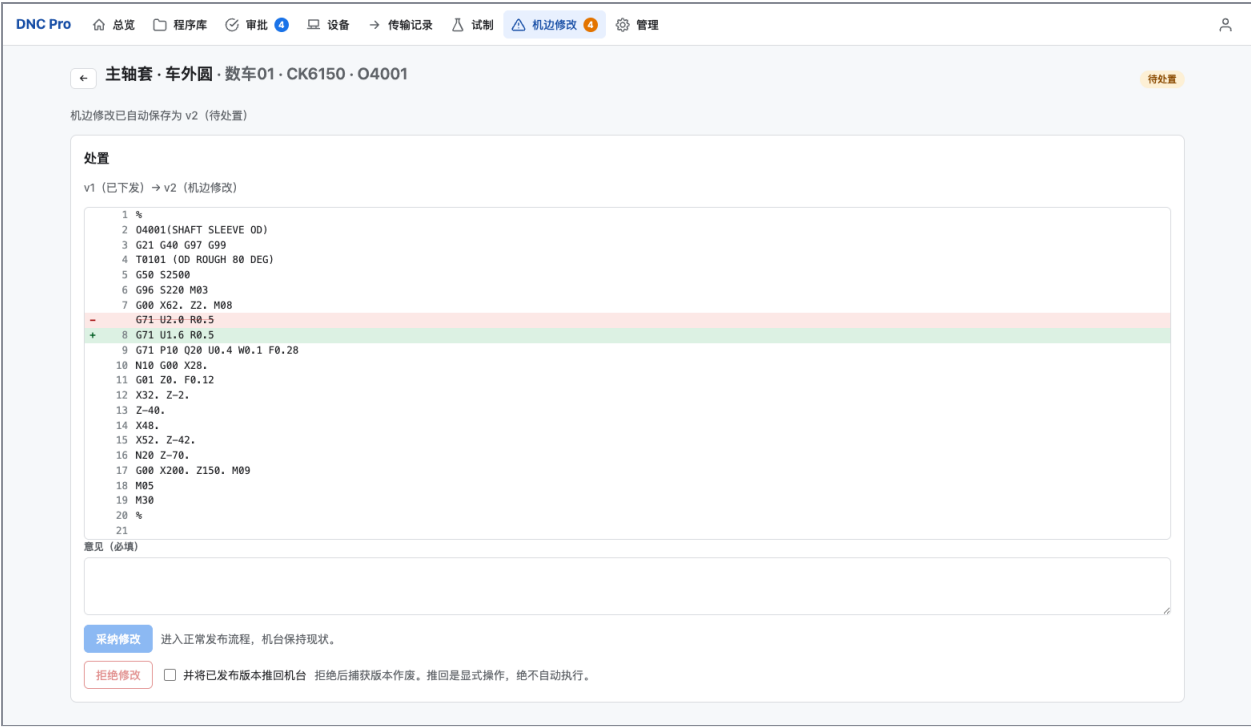


图 2-4 机边修改的差异比对

图 2-4 中，操作工将 G71 的每刀切深由 2.0 mm 改为 1.6 mm。采纳后该版本进入正常发布流程。完整规则见 5.7。

2.5 场景四：试制程序遗留在机床上

失效表现。 试制版本未被撤回，次日班次将其当作正式程序批量加工。

本系统的措施。 试制为显式的限时操作。下发时勾选「试制」并设定时长后，该机台上的该文件在全部界面上带「试制中」徽标；到期后状态转为「已过期」并继续显示，由人员决定转正（走正式发布流程）或撤回（推回上一版受控内容）。

机组级可整体停用试制，用于不允许出现试制程序的量产节拍机。完整规则见 5.5。

2.6 场景五：控制器数据丢失

失效表现。 电池失效、参数丢失或控制器换板导致机床上的全部程序丢失，其中多数为历年积累、未纳入任何文件管理体系的机床本地程序。

本系统的措施。 滚动镜像全天候备份机床上的每一个文件，不限于受管程序。未受管文件同样保有历史快照并可还原，但不被检查也不被纠正，仅受到保护。



图 2-5 机台详情页面中并列的受管文件与未受管文件

未受管文件可随时采纳进程序库，亦可保持未受管状态继续受到备份保护。完整规则见 5.6。

2.7 场景六：无法回答追溯问题

失效表现。 客户投诉一批零件尺寸超差，需要回答该批次使用的程序版本、审批人、下发时间与目标机台，现有记录无法支撑。

本系统的措施。 只增不改的哈希链审计日志记录每一次状态变更（版本创建、提交、批准、下发请求、下发完成、机边修改捕获与处置等）与每一次程序内容外流（正文的查看与下载）。日志可按操作者、机台、对象、时间段查询，支持导出 CSV 与哈希链完整性校验。

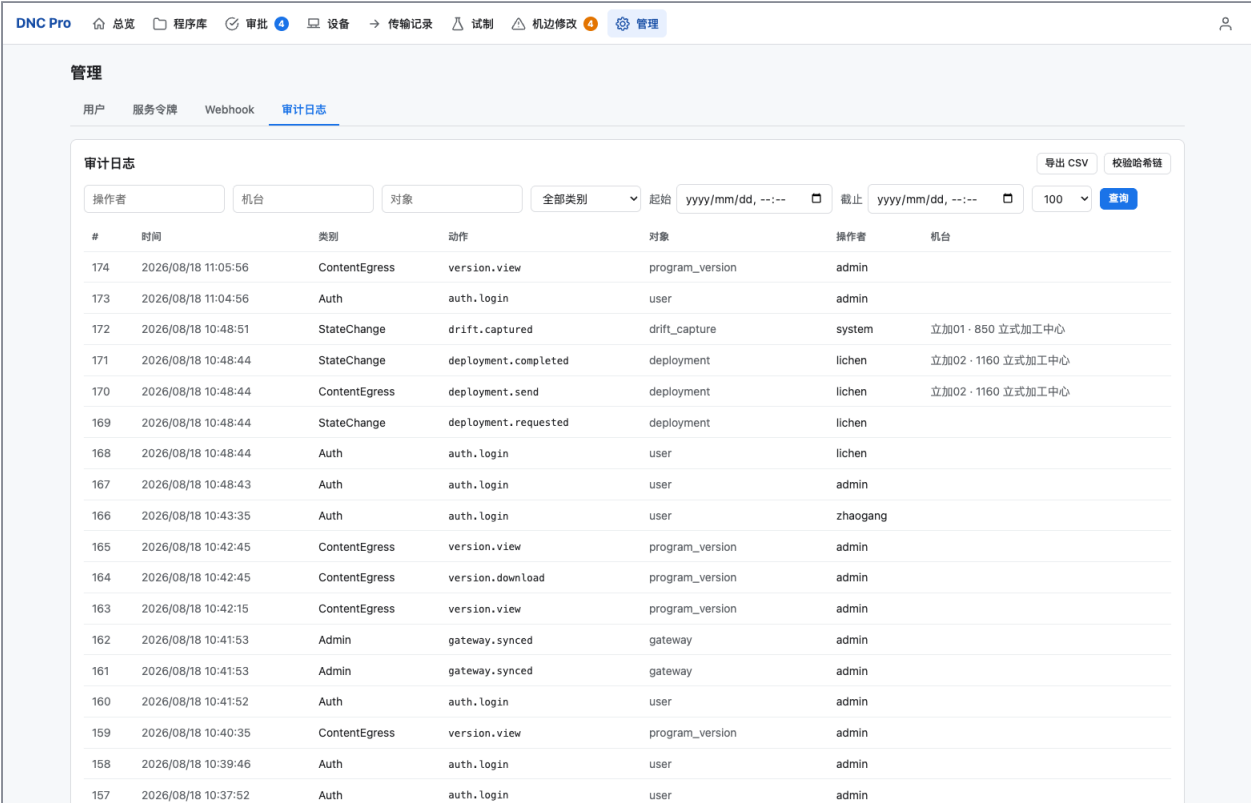


图 2-6 审计日志页面

完整规则见 5.9。

2.8 接口一致性

管理控制台与机边操作台均为同一套 REST API 的客户端，不存在未公开接口。MES 自动创建工单对应的下发任务、CAM 后处理自动上传新版本、看板订阅下发结果等集成需求，使用与界面相同的接口与相同的权限规则实现。

接口定义见 6.3。

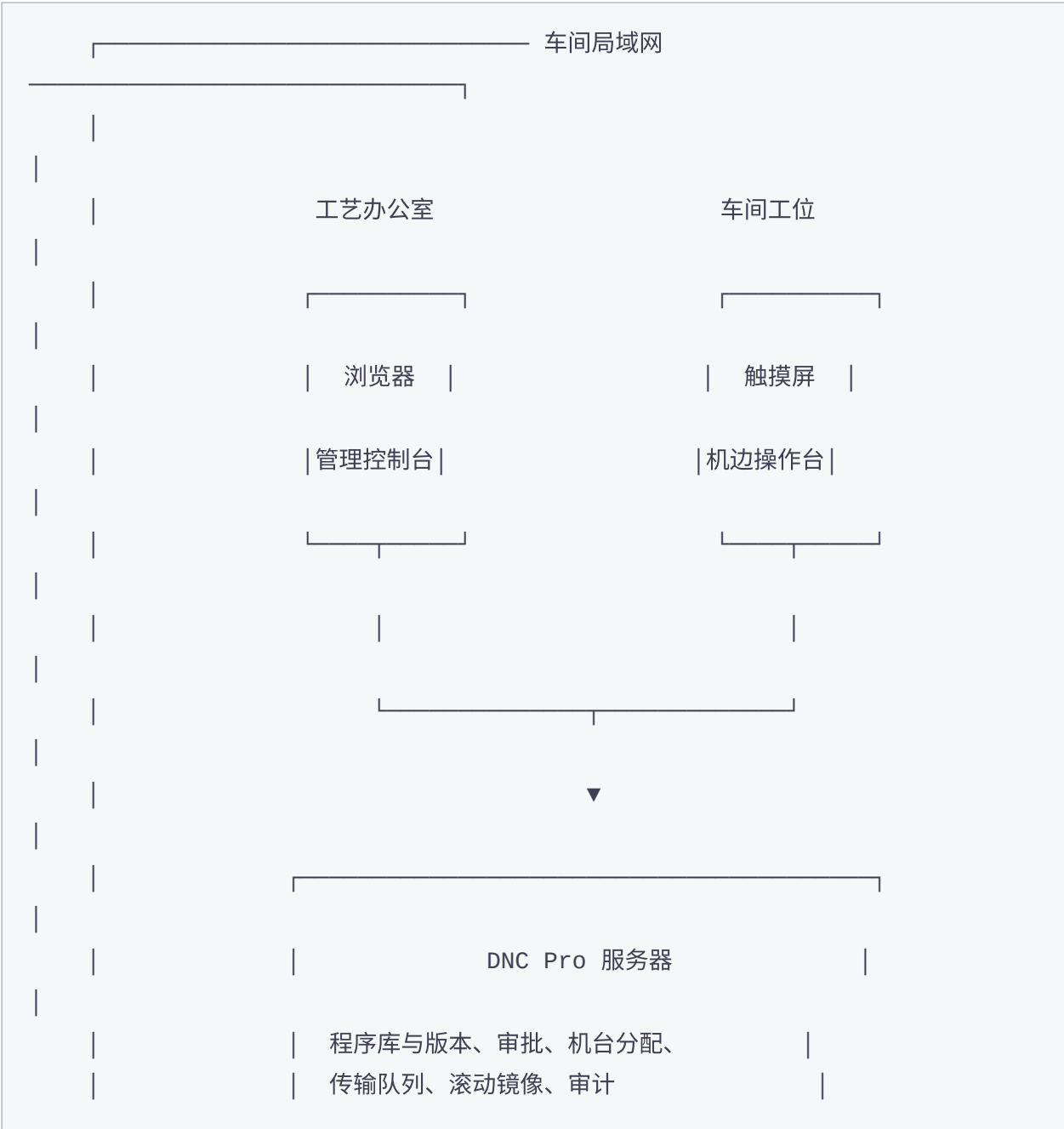
3 系统构成

3.1 适用范围

本章说明 DNC Pro 系统由哪些部分构成、各部分之间如何连接、后台持续运行哪些机制，用于理解界面上所见行为的由来，以及使用中的故障定位。

3.2 系统构成

系统的组成与连接关系见图 3-1。



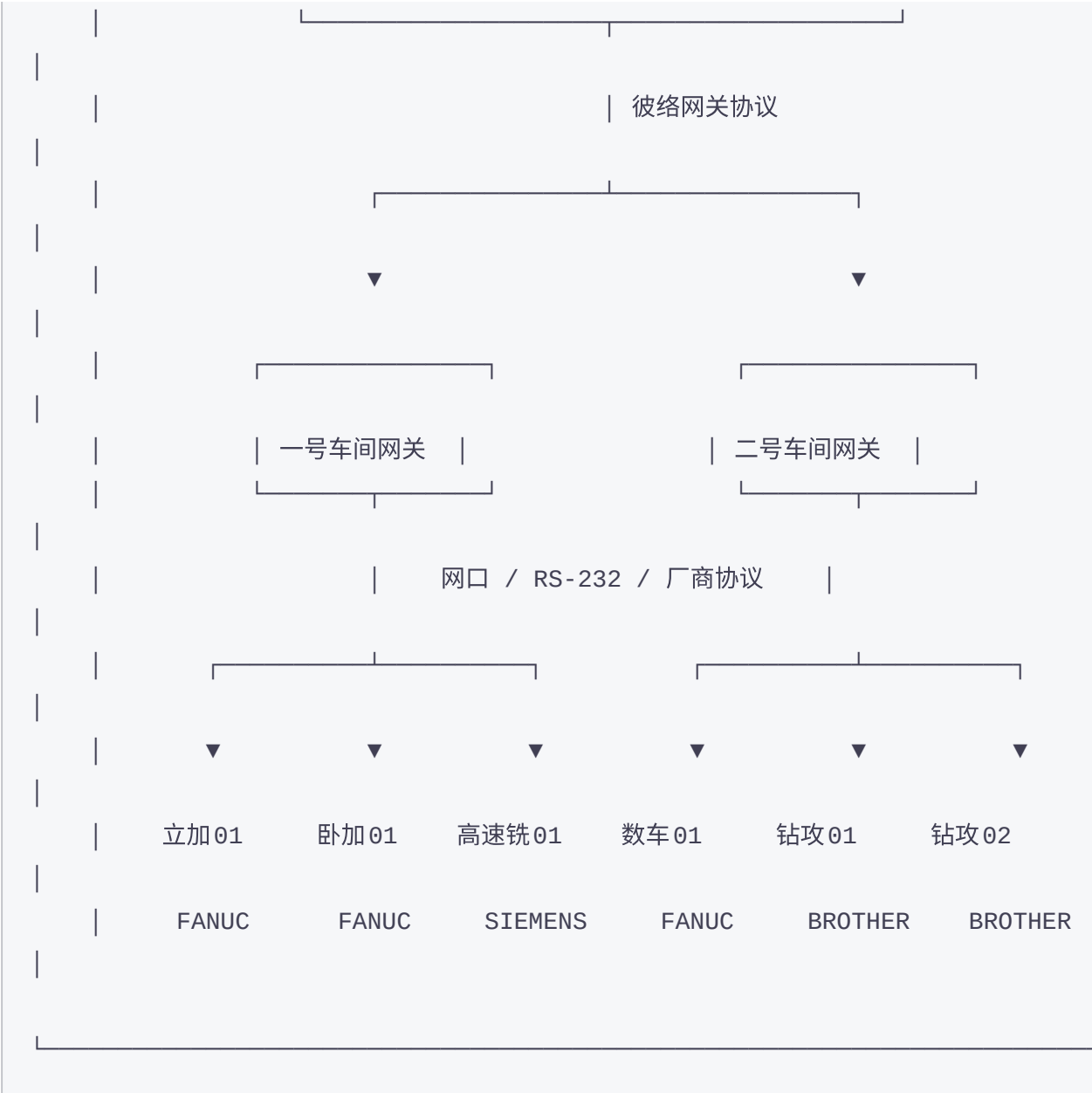


图 3-1 系统构成与连接关系

使用人员经浏览器或车间触摸屏访问本系统，访问地址见 4.0.2。整套系统运行于使用单位的局域网内，不需要外网连接。

本系统不直接连接机床。与机床的全部通信经由彼络物联网关的 HTTP 协议完成，包括列目录、读文件、写文件、删文件、读取当前运行程序等操作。该设计带来两项结果：

- a) 厂商差异由网关吸收。FANUC、西门子、三菱、兄弟的文件系统语义差异较大，网关已将其统一为一套接口，本系统的处理差异见 6.2；
- b) 一套本系统可管理多个车间。每个车间部署一台网关，本系统侧仅增加一条网关记录。

程序正文按内容哈希存放，内容相同的版本天然去重，因此保存完整的历史快照并不会带来成倍的存储占用，见 5.6.9。

3.3 后台机制

本系统后台持续运行三项互不阻塞的机制。各机制的周期决定界面数据的更新时机。

3.3.1 传输执行器

自传输队列取出任务，对单台机台串行执行事务式下发（见 5.4）。处于下发中的机台不会同时被镜像读取，滚动镜像始终向真实传输让路。

3.3.2 滚动镜像调度

持续轮转扫描整个机队。每台网关同一时刻仅扫描一台机床，请求之间设有节流间隔，一轮扫完后短暂休眠再重新开始。执行规则如下：

- a) 跳过当前正在运行的程序；
- b) 每成功完整扫完一台机床后，更新该机台的「最近校验」时刻；
- c) 扫描失败时记录到该机台并在控制台显示，不仅写入日志。

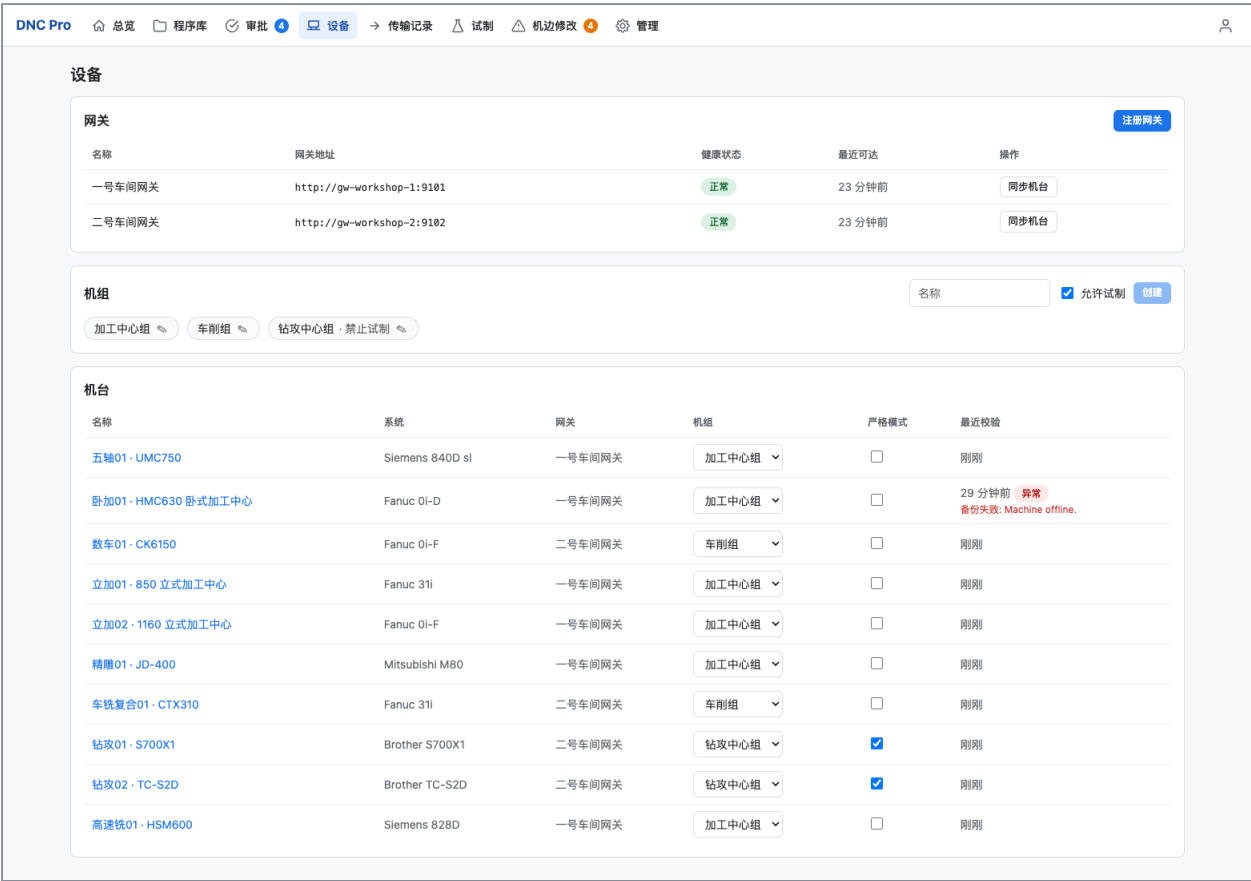


图 3-2 设备页面显示的镜像失败原因

图 3-2 中，卧加 01 的镜像失败原因（备份失败：Machine offline.）直接显示在行内。完整规则见 5.6。

3.3.3 试制到期扫描

每分钟将超时的「试制中」记录标记为「已过期」。

注意

到期扫描仅改变状态标记，不改动机床上的内容。撤回与转正均须由人员执行， 见 5.5。

3.4 数据流转

一个版本的完整流转见图 3-3。

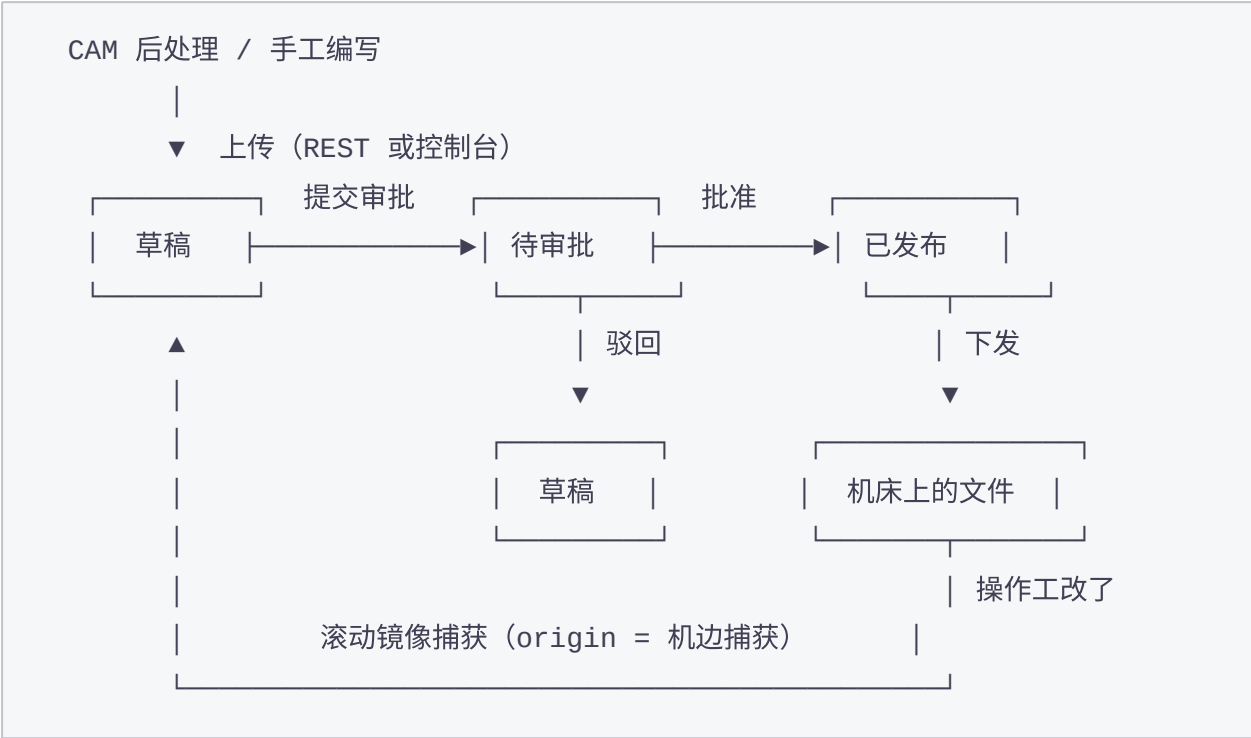


图 3-3 版本的数据流转

同一流程亦适用于采纳：机床上原本未受管的文件可采纳进指定程序库，以采纳基线作为 v1 纳入受控管理，见 5.6。

3.5 与彼络物联网关的职责划分

表 3-1 与网关的职责划分

事项	网关负责	本系统负责
与机床通信（协议、编码、超时、重连）	√	×
采集产量、OEE、报警、刀具数据	√	×
程序版本、审批、权限	×	√
下发的事务性与回读校验	×	√
全机队滚动备份与历史快照	×	√
审计与合规追溯	×	√

网关自带的程序传输页面仍可使用，适用于调试与一次性操作。本系统是其受控上层。

接入与初始配置见第 4 章。

4 接入与初始配置

本章规定 DNC Pro 系统交付完成后，自接入车间网关到首个程序成功下发并通过回读校验的 完整实施过程。全过程约需 20 分钟。

说明

本章自使用单位取得访问地址与管理员账号之后开始。

实施步骤按表 4-1 的顺序执行。

表 4-1 实施步骤

步骤	内容	实施人员
4.1 接入网关与机台	在网关侧建立账号、在本系统注册网关、同步机台、划分机组	设备管理人员
4.2 首次程序下发	建立程序库、程序、上传版本、审批放行、绑定机台、执行下发	工艺工程师

实施前应完整阅读安全与注意事项。

4.0.1 先决条件

开始实施前应逐项确认下列条件：

- a) 本系统已完成交付并处于运行状态，使用单位已取得访问地址与管理员账号；
- b) 本系统与车间网关之间网络可达，网关 HTTP 服务监听 80 端口；
- c) 网关侧已存在可用的登录账号，且实施人员掌握其「设置 → 用户管理」的操作方法；
- d) 车间的浏览器与触摸屏可访问本系统的地址。

注意

交付时提供的管理员初始密码应在首次登录后立即经「右上角账户菜单 → 修改密码」更换。

4.0.2 访问地址

在浏览器中打开管理控制台地址进入登录页面。

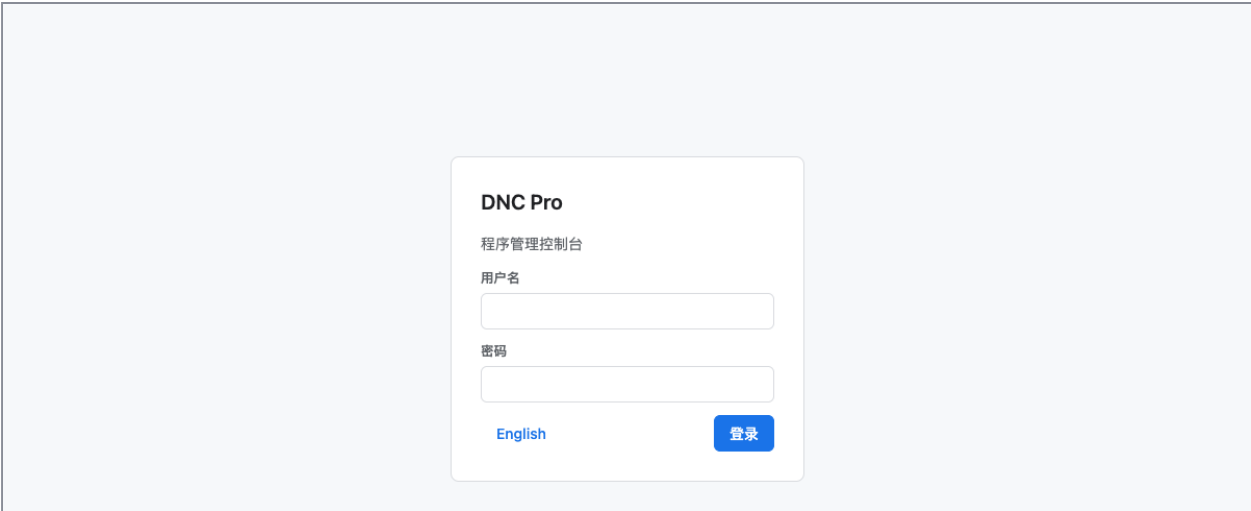


图 4-1 管理控制台登录页面

本系统对外提供的地址按表 4-2 的规定，其中 <主机> 为交付时确定的主机地址或域名。

表 4-2 访问地址

地址	用途
http://<主机>:8030/	管理控制台
http://<主机>:8030/shopfloor/	机边操作台（车间触摸屏）
http://<主机>:8030/api/docs	REST API 交互式参考
http://<主机>:8030/openapi/v1.json	OpenAPI 3.1 文档

说明

8030 为默认端口，交付时可能另行约定，应以实施人员提供的地址为准。

4.0.3 演示环境说明

本说明书的截图取自一套可复现的演示数据集，其构成如下：

- a) 两台车间网关（一号车间网关、二号车间网关），后者启用密钥认证；
- b) 10 台机床，覆盖 FANUC 3li / 0i-F / 0i-D、SIEMENS 828D / 840D sl、Mitsubishi M80、Brother S700X1 / TC-S2D 共七种控制系统组合；
- c) 三个程序库，分别采用单人审批、自动放行、双人会签三套审批策略；
- d) 六名不同角色、不同授权范围的人员；

e) 一批已执行完成的下发记录（含一次失败并自动回滚）、两项进行中的试制、四条待处置的机边修改。

演示环境不连接真实机床，全部机床由模拟网关提供，可完整演练本说明书描述的全部流程。需要演示环境时应向供应方申请。

注意

演示数据集中的账号与口令为公开示例值，不应用于生产环境。真实环境应使用交付时提供的管理员账号登录，并按 4.0.1 的规定立即修改密码。

4.1 接入网关与机台

4.1.1 适用范围

本节规定彼络物联网网关的接入方法与机台台账的建立方法。适用于设备管理人员与管理员。

本系统经由网关与机床通信，不直接连接机床。

4.1.2 建立网关专用账号

注意

不应使用网关的管理员账号供本系统直连。管理员账号的口令变更会影响其他用途，且操作责任无法区分。

操作步骤：

- a) 打开网关界面，进入「设置 → 用户管理」，新建一个专供本系统使用的用户；
- b) 在该用户的「用户安全」中生成 Secret Key；
- c) 保持网关的安全控制处于启用状态。

详细步骤见网关说明书·设置。

4.1.3 注册网关

操作步骤：进入「设备 → 注册网关」，按表 4-3 的规定填写各字段并保存。

表 4-3 网关注册字段

字段	填写要求
名称	车间内通用的称谓，例如 一号车间网关
网关地址	http://<网关IP>，网关 HTTP 服务监听 80 端口
认证方式	密钥（推荐，填入 4.1.2 生成的 Secret Key）、用户名密码，或 无（仅限完全隔离的可信网段）

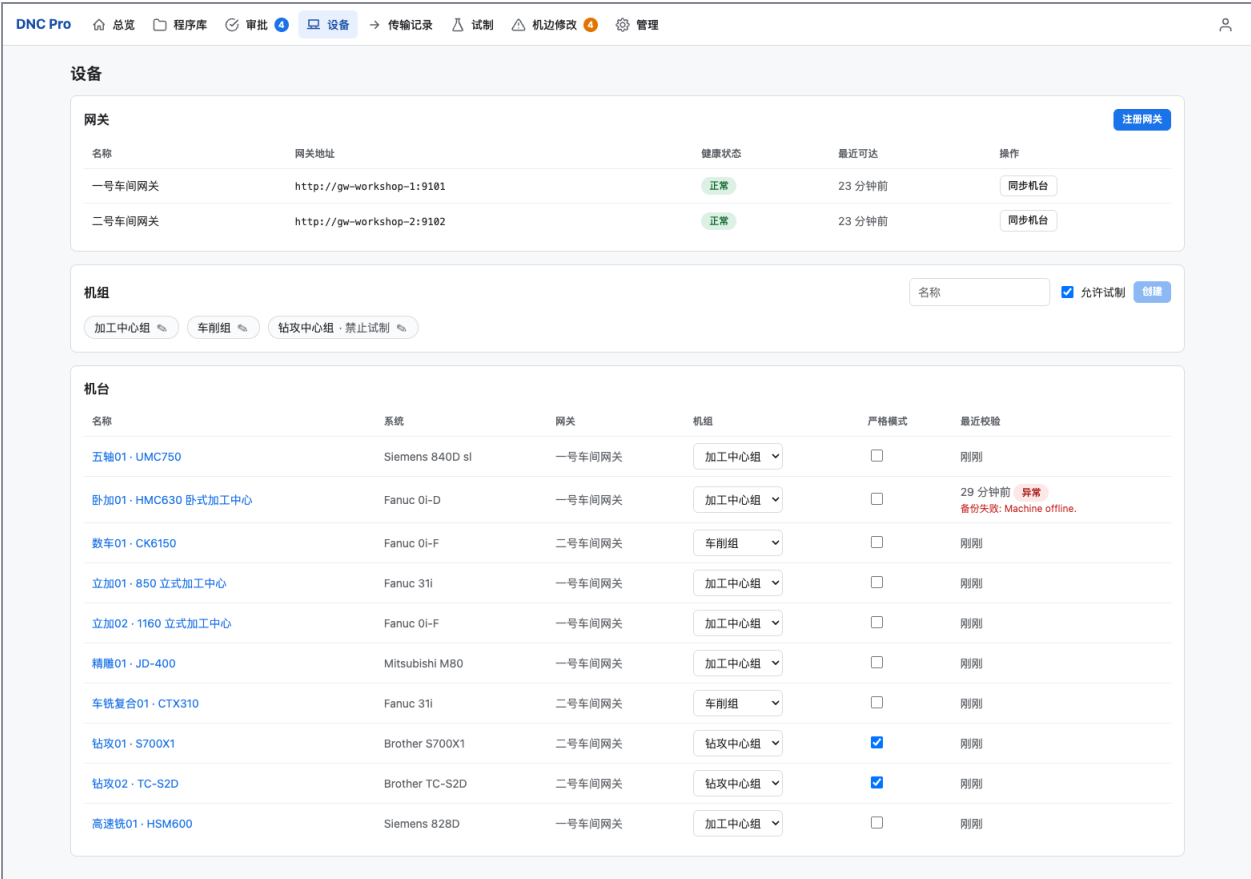


图 4-2 设备页面的网关列表

图 4-2 中共注册两台网关，一台位于可信网段采用无认证方式，另一台采用密钥认证。

说明

网关行的「最近可达」记录最近一次成功同步的时刻，不是心跳时刻。判定机床当前是否处于正常备份状态应查看机台行的「最近校验」，该值由滚动镜像持续更新，见 5.6。

注意

网关凭据以加密形式存储，不在任何界面或 API 响应中回显。更换密钥时应重新注册一台网关，原网关停用。

4.1.4 同步机台台账

操作步骤：在目标网关行单击「同步机台」。

系统读取网关的机床配置并更新台账，处理规则如下：

- a) 新增：网关上存在、本系统中不存在的机床；
- b) 更新：名称、控制系统、型号、IP、编码、文件根目录等属性发生变化的机床；

c) **孤立**：曾同步过、但本次网关配置中不存在的机床。系统保留其历史记录， 不再对其执行任何操作。

同步操作具备幂等性，可随时重复执行。机床增减或改名后应重新执行一次同步。

4.1.5 划分机组

机组是授权与策略的施加单位，不表示物理位置。机组决定下列两项：

- a) 可操作该组机床的人员范围。权限可按机组授予，见 6.1；
- b) 该组机床是否允许试制。该项为机组级开关，见 5.5。

演示环境的机组划分按表 4-4 的规定。

表 4-4 演示环境的机组划分

机组	所含机台	允许试制
加工中心组	立加 01/02、卧加 01、高速铣 01、五轴 01、精雕 01	√
车削组	数车 01、车铣复合 01	√
钻攻中心组	钻攻 01、钻攻 02	×

钻攻中心为量产节拍机，不允许出现试制程序。该策略由机组开关强制执行，不依赖人员记忆。

4.1.6 机台级选项

在设备页的机台表中按行设置，选项按表 4-5 的规定。

表 4-5 机台级选项

选项	含义
机组	该机台归属的机组，决定授权范围与试制策略
严格模式	在该机台的文件列表中高亮标记未受管文件。仅作参考提示，不阻断任何操作

严格模式适用于不允许出现计划外程序的机台，其作用是标出待核查项，不是阻断操作。

4.1.7 接入结果验证

同步完成后不执行任何其他操作，等待 1~2 分钟后返回设备页，按下列各项核对：

- a) 每台机床的「最近校验」应由空白变为「刚刚」，表明滚动镜像已完成一轮扫描；
- b) 进入任一机台详情页，应能看到该机床上已有的文件，且全部标记为「未受管」。



图 4-3 接入后的机台文件列表

图 4-3 中，机床上原有的文件均为未受管状态：已被备份，但不受任何策略约束。纳入受控管理的方法见 5.6。

某机台的「最近校验」持续不更新时，行内显示具体失败原因（例如 备份失败：Machine offline.）。常见原因与处理措施见 7.2。

接入完成后按 4.2 执行首次程序下发。

4.2 首次程序下发

4.2.1 适用范围

本节规定一条完整链路的实施步骤：建立程序库、建立程序、上传版本、审批放行、绑定机台、执行下发、机边确认。适用于工艺工程师。

本节的目的是验证系统各环节已正确配置，不得省略其中任一步骤。

4.2.2 前置条件

- a) 系统已完成交付并处于运行状态，实施人员可以管理控制台的账号登录；
- b) 网关已按 4.1 接入，机台台账已同步，机组已划分；
- c) 实施人员具备编程员权限，并可协调一名具备审批员权限的人员配合。

4.2.3 建立程序库

操作步骤：进入「程序库 → 新建程序库」，按需配置审批策略。

程序库是审批策略的施加单位。一个车间通常需要 2~3 个程序库，典型配置按表 4-6 的规定。

表 4-6 典型程序库配置

程序库	审批人数	禁止自审自批	自动放行	适用范围
量产程序库	1	启用	停用	已量产零件，内容改动须经第二人复核
试制程序库	1	停用	启用	新品试制期，需快速迭代
工装与对刀库	2	启用	停用	全部机床共用的宏与子程序，影响面较大

三项参数的含义：

- a) **审批人数**：放行所需的不同审批人数量；
- b) **禁止自审自批**：作者本人不得批准自己创建的版本，默认启用；

c) **自动放行**：版本提交后直接发布，不进入审批队列。

注意

「禁止自审自批」为系统默认配置，用于阻断「修改后随手放行」这一类最常见的差错来源。仅配备一名工程师的单位应改用自动放行，不应保留形式上的多人审批配置。

4.2.4 建立程序并上传首个版本

操作步骤：

- a) 进入「程序库 → 新建程序」，按表 4-7 的规定填写各字段；
- b) 在程序详情页单击「上传新版本」，选择文件；
- c) 填写版本备注，保存。

表 4-7 程序身份字段

字段	填写要求	示例
名称	人员识别用的名称	泵体 · 粗铣外形
零件号	图号或料号	HX-2043
工序	工序号	OP10
适用机型	提示性信息，用于选择机台	FANUC 31i、FANUC 0i-F
说明	该程序的加工内容	—

说明

版本备注是后续追溯的直接依据，应记录改动内容与理由，例如「切深 2.5→3.0 mm，走刀 300→260，配合新牌号刀片提效」。仅填写「改了参数」不具备追溯价值。

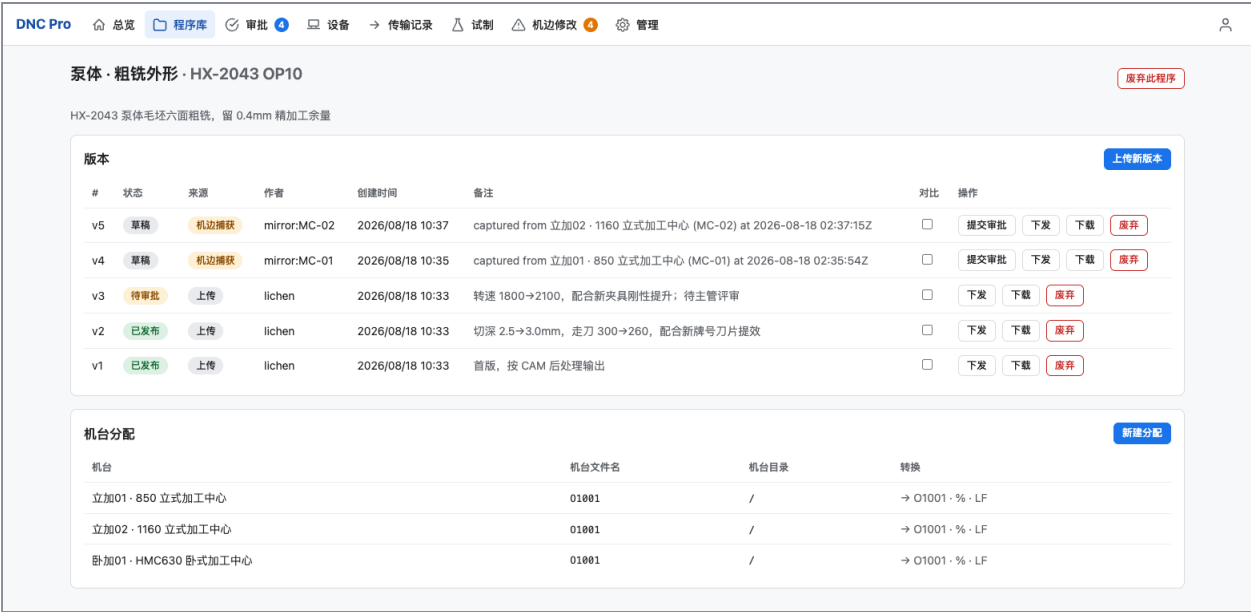


图 4-4 程序详情页面

上传后版本处于「草稿」状态，仅作者与具备相应权限的人员可见，不允许下发。

4.2.5 提交审批并放行

操作步骤：

- a) 在版本行单击「提交审批」，版本转为「待审批」；
- b) 由具备 审批员 角色的人员在「审批」页单击「审阅」；
- c) 核对差异，填写审批意见（必填），单击「批准」。

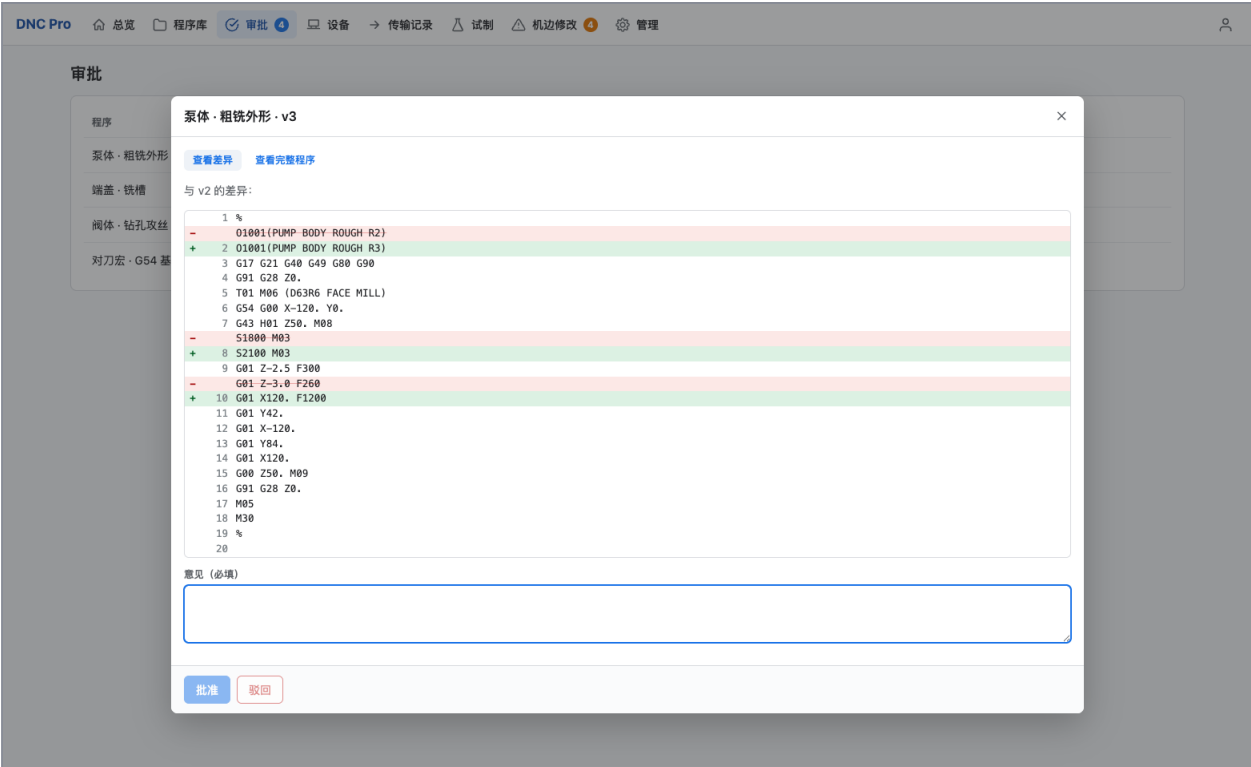


图 4-5 审批评审弹窗

评审弹窗默认展示与上一版本的差异，可切换至「查看完整程序」。

批准后的结果：

- a) 已达到程序库要求的审批人数时，版本转为「已发布」，可执行下发；
- b) 未达到时保持「待审批」，界面显示已获得的批准次数。

驳回的版本退回「草稿」，由作者修改后重新提交。完整规则见 5.2。

说明

查看程序正文构成一次内容外流，系统记录一条 `version.view` 审计记录。该记录用于在追溯时回答程序内容的流向问题，见 5.9。

4.2.6 绑定机台

一条机台分配规定该程序下发至指定机床时的落地文件名、落地目录与落地转换。

操作步骤：进入程序详情页 → 「机台分配 → 新建分配」，按表 4-8 的规定填写。

表 4-8 机台分配字段

字段	填写要求
机台	目标机床
机台文件名	机床上的文件名，FANUC 用 01001，西门子用 DG3320_OP20.MPF
机台目录	留空时使用该机床的文件根目录
转换	落地前对内容执行的处理，按表 4-9 的规定

表 4-9 落地转换项

转换项	作用
程序名改写	将内容中的程序名行改写为目标名称。FANUC 系统必设
保证 % 包裹	在内容首尾补 % 行
行结束符	设为 LF 或 CRLF
目标编码	机床侧的字符编码

警告

FANUC 控制器忽略传入的文件名参数，程序名取自内容中第一个与第二个换行符之间的一行（01001(PUMP BODY ROUGH) 或 <NAME> 形式）。向 FANUC 机床建立分配时必须设置「程序名改写」为目标 O 号，否则程序将以内容中原有的号落地，导致后续下发覆盖非预期的程序号。详见 5.3 与 6.2。

分配建立后应执行「预览转换」，核对将发送至机床的字节内容及其 SHA-256 值。该值应与后续下发记录中的「转换后哈希」完全一致。

4.2.7 执行下发

操作步骤：

- a) 在已发布的版本行单击「下发」；
- b) 勾选目标分配，可多选以批量下发至多台机床；
- c) 选择正式下发或试制下发（试制规则见 5.5）；
- d) 确认执行。

警告

下发将删除机床上的目标文件后重新写入。执行前应确认目标机床未处于加工状态，且目标程序未被机床调用。

下发任务进入队列，由系统后台串行执行事务式传输。在「传输记录」页查阅各条记录的状态。

DNC Pro

总览

程序库

审批

设备

传输记录

试制

机边修改

管理

传输记录

刷新

机台全部机台

状态全部状态

共 16 条, 0 进行中, 1 失败

机台	文件	状态	失败阶段	回滚	试制	排队时间	完成时间
立加02 · 1160 立式加工中心	09002	成功 (已校验)				2026/08/18 10:48:44	2026/08/18 10:48:44
钻攻01 · S700X1	01100	成功 (已校验)				2026/08/18 10:37:14	2026/08/18 10:37:14
精雕01 · JD-400	07002	成功 (已校验)			试制	2026/08/18 10:35:45	2026/08/18 10:35:45
五轴01 · UMC750	SJ9001_0P10.MPF	成功 (已校验)			试制	2026/08/18 10:35:44	2026/08/18 10:35:44
车铣复合01 · CTX310	06001	失败 send failed: Network fault.	发送	已回滚		2026/08/18 10:35:44	2026/08/18 10:35:44
高速铣01 · HSM600	DG3320_0P20.MPF	成功 (已校验)				2026/08/18 10:35:35	2026/08/18 10:35:35
数车01 · CK6150	04001	成功 (已校验)				2026/08/18 10:35:34	2026/08/18 10:35:34
钻攻02 · TC-S2D	01100	成功 (已校验)				2026/08/18 10:35:34	2026/08/18 10:35:34
钻攻01 · S700X1	01100	成功 (已校验)				2026/08/18 10:35:34	2026/08/18 10:35:34
立加01 · 850 立式加工中心	01002	成功 (已校验)				2026/08/18 10:35:33	2026/08/18 10:35:33
卧加01 · HMC630 卧式加工中心	09002	成功 (已校验)				2026/08/18 10:35:33	2026/08/18 10:35:33
立加02 · 1160 立式加工中心	09002	成功 (已校验)				2026/08/18 10:35:33	2026/08/18 10:35:33
立加01 · 850 立式加工中心	09002	成功 (已校验)				2026/08/18 10:35:33	2026/08/18 10:35:33
卧加01 · HMC630 卧式加工中心	01001	成功 (已校验)				2026/08/18 10:35:32	2026/08/18 10:35:32
立加02 · 1160 立式加工中心	01001	成功 (已校验)				2026/08/18 10:35:32	2026/08/18 10:35:32
立加01 · 850 立式加工中心	01001	成功 (已校验)				2026/08/18 10:35:32	2026/08/18 10:35:32

图 4-6 传输记录页面

状态为「成功（已校验）」表示机床上的当前内容经回读后与发送内容逐字节一致（已按厂商画像归一化）。仅在该状态下方可通知操作工启动加工。事务阶段与失败处置见 5.4。

4.2.8 机边确认

操作步骤：

- a) 打开机边操作台 <http://<主机>:8030/shopfloor/>，使用操作工账号登录；
- b) 选定目标机床；
- c) 核对程序卡片的状态标识为「机床上已是最新版本」。



图 4-7 机边操作台的机台页面

至此完成一条完整链路：上传 → 审批 → 发布 → 分配 → 下发 → 回读校验 → 机边确认。

4.2.9 后续内容

- a) 多版本管理、版本比对与废弃见 5.1;
- b) 机床侧改动的处置见 5.7;
- c) 上述步骤的岗位分工与授权配置见 6.1。

5 操作说明

本章规定 DNC Pro 系统投入使用后的日常操作方法。各节的编排顺序与程序的实际流转顺序一致：程序库与版本（5.1）→ 审批与放行（5.2）→ 机台分配（5.3）→ 程序下发（5.4）， 其余各节为在此主线上展开的专项操作。

接入与初始配置见第 4 章；角色、权限、机床差异与接口定义见第 6 章。

5.0.1 按角色索引

表 5-1 按角色索引

岗位（系统角色）	承担的操作	相关条款
工艺工程师（程序员）	上传版本、提交审批、绑定机台、下发、处置机边修改	5.1、5.2、5.3、5.4、5.7
工艺主管（审批员）	审阅版本差异，批准或驳回	5.2
操作工	在机边操作台核对版本并按需下发	5.8
设备管理人员	维护网关与机台台账，监视滚动镜像	4.1、5.6
系统管理员	用户与授权、服务令牌、Webhook、审计核查、日常核查	5.9、6.4

5.0.2 按场景索引

表 5-2 按场景索引

场景	相关条款
程序内容变更，需发布新版本	5.1 → 5.2
新机床上线，需建立程序与机台的对应关系	5.3
下发失败，需确认机床上的实际内容	5.4
新品试制，需限制程序在机床上的留存时间	5.5
操作工在机床侧修改了程序	5.7
机床控制器数据丢失，需还原程序	5.6
机床上存在大量未纳入管理的历史程序	5.6
需回答某批零件使用的程序版本与审批人	5.9

场景	相关条款
与 MES、CAM 等上层系统对接	5.9 → 6.3

5.1 程序库与版本

5.1.1 适用范围

本节规定加工程序在本系统中的组织方式、版本状态的流转规则，以及版本内容的比对与取出方法。适用于程序员、审批员与管理员。

5.1.2 对象层次

本系统按程序库、程序、版本三层组织加工程序，层次关系见图 5-1。

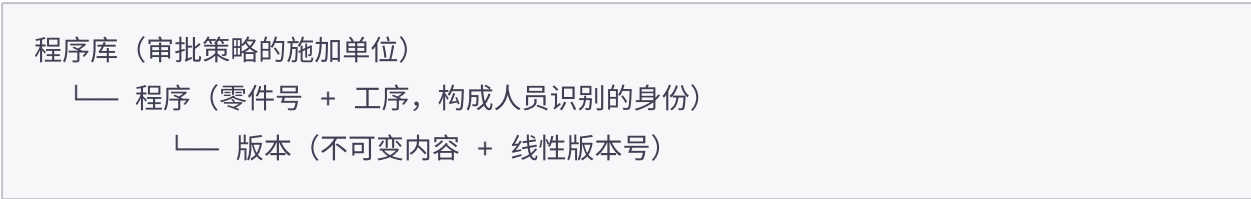


图 5-1 程序库、程序、版本的层次关系

各层的职责如下：

- a) 程序库规定其下程序所需的审批人数、能否自审自批、是否自动放行；
- b) 程序规定身份信息，包括名称、零件号、工序、适用机型与说明；
- c) 版本承载内容。版本内容在上传后不可更改，可变更的仅为其状态。



图 5-2 程序库页面

程序库页面支持按程序库筛选，按名称、零件号、工序检索。「已发布版本」列显示当前执行下发时将发出的版本号。

5.1.3 版本状态

版本状态的流转按图 5-3 的规定执行，各状态的允许操作按表 5-3 的规定。

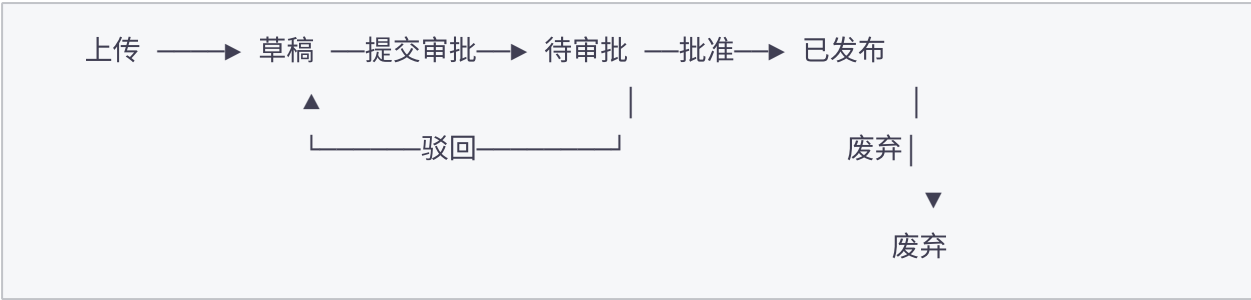


图 5-3 版本状态转换

表 5-3 版本状态与允许操作

状态	允许的操作	限制
草稿	提交审批、废弃	不允许下发
待审批	由审批人批准或驳回	作者可查阅，不得自行改为已发布
已发布	下发至机台	同一程序可同时存在多个已发布版本，下发时须指定版本号
废弃	查阅历史	不出现在可下发列表中

程序整体亦可废弃，用于该程序退役的情形。废弃的程序默认不在列表中显示。

5.1.4 版本来源

版本行的「来源」标签标明该版本的产生方式，是追溯的关键依据，取值按表 5-4 的规定。

表 5-4 版本来源

来源	产生方式
上传	由人员从 CAM 系统或编辑器上传
机边捕获	滚动镜像发现受管文件在机床侧被改动后自动捕获（见 5.6）
采纳	机床上原本未受管的文件被采纳进程序库时建立的基线（见 5.6）

DNC Pro

总览

程序库

审批

设备

传输记录

试制

机边修改

管理

泵体·粗铣外形·HX-2043 OP10

废弃此程序

HX-2043 泵体毛坯六面粗铣，留 0.4mm 精加工余量

版本

上传新版本

#	状态	来源	作者	创建时间	备注	对比	操作
v5	草稿	机边捕获	mirror:MC-02	2026/08/18 10:37	captured from 立加02·1160 立式加工中心 (MC-02) at 2026-08-18 02:37:15Z	☐	提交审批 下发 下载 废弃
v4	草稿	机边捕获	mirror:MC-01	2026/08/18 10:35	captured from 立加01·850 立式加工中心 (MC-01) at 2026-08-18 02:35:54Z	☐	提交审批 下发 下载 废弃
v3	待审批	上传	lichen	2026/08/18 10:33	转速 1800→2100，配合新夹具刚性提升；待主管评审	☐	下发 下载 废弃
v2	已发布	上传	lichen	2026/08/18 10:33	切深 2.5→3.0mm，走刀 300→260，配合新牌号刀片提效	☐	下发 下载 废弃
v1	已发布	上传	lichen	2026/08/18 10:33	首版，按 CAM 后处理输出	☐	下发 下载 废弃

机台分配

新建分配

机台	机台文件名	机台目录	转换
立加01·850 立式加工中心	01001	/	→ O1001·%·LF
立加02·1160 立式加工中心	01001	/	→ O1001·%·LF
卧加01·HMC630 卧式加工中心	01001	/	→ O1001·%·LF

图 5-4 程序详情页面的版本列表

说明

机边捕获的版本进入系统时状态为草稿。该版本已被安全保存，但尚不具备任何效力，须由工程师在机边修改页面处置，见 5.7。

5.1.5 内容去重与内容哈希

版本内容按 SHA-256 值寻址存储，内容完全一致的版本在底层仅存储一份。滚动镜像每日为全部机台产生的快照中绝大多数为重复内容，因此不显著增加存储占用。

版本详情中的内容哈希是排查内容一致性问题的判定依据，可与传输记录中的「转换后哈希」与「回读哈希」逐一对照。

5.1.6 版本比对

操作步骤：

- a) 在版本表最右侧的「对比」列勾选任意两个版本；
- b) 界面给出并排差异视图，删除行标红，新增行标绿；
- c) 审批准审弹窗默认展示待审批版本与其上一版本的差异。

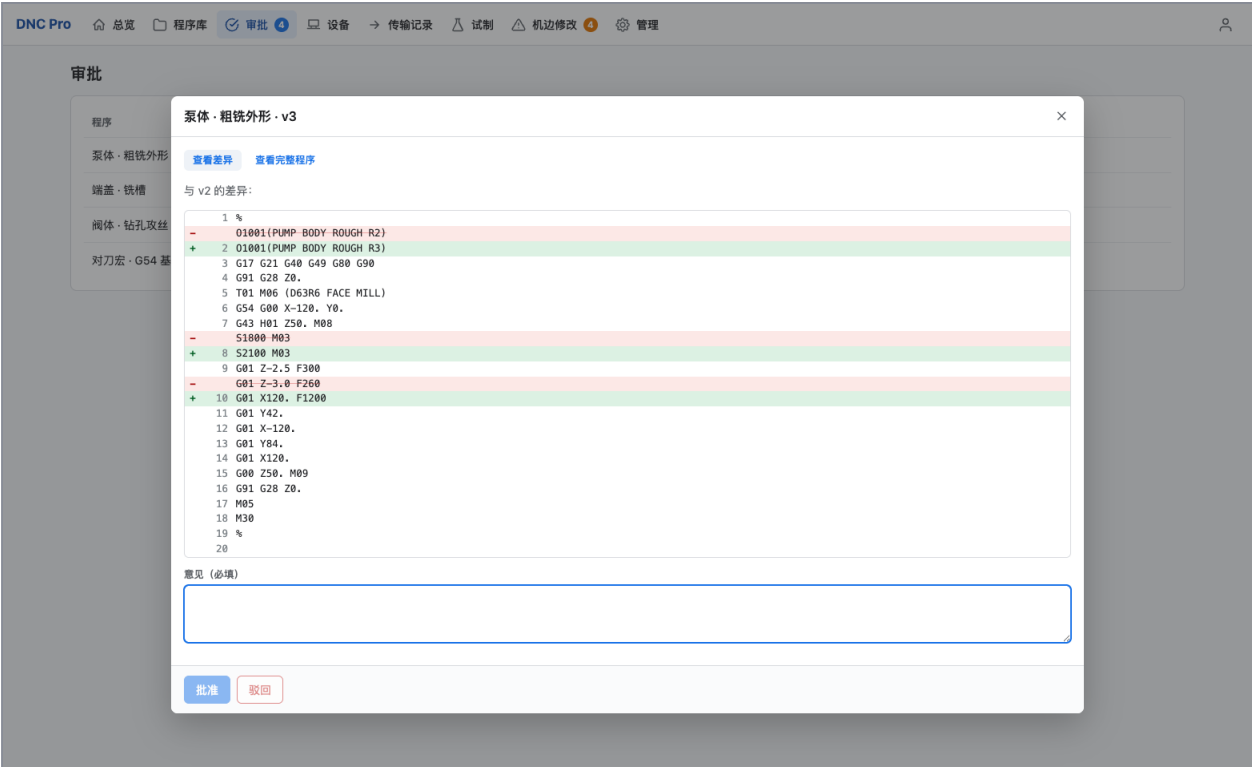


图 5-5 版本差异对比视图

5.1.7 变体分组

零件号与工序相同、但因机床控制系统不同而分别编制的多个程序（例如 FANUC 版与西门子版），由本系统以 零件号::工序 作为变体分组键在界面上归组显示。

注意

变体分组仅影响界面显示。同一分组内的程序仍为相互独立的程序，各自保有独立的版本历史与审批记录，系统不对其内容作任何合并或同步。

5.1.8 内容下载与外流记录

版本行的「下载」按钮取出该版本的原始内容。

每一次正文查看或下载均写入一条 version.view 审计记录，记录操作人、时间、来源 IP 与版本号。该记录用于回答程序内容的流向问题，不构成对查看行为的限制。审计查询方法见 5.9。

5.1.9 权限要求

表 5-5 程序库相关权限

操作	所需权限	具备该权限的角色
查阅程序列表与元数据	programs.read	程序员、审批员、只读、管理员
查阅正文、下载内容	programs.content.view	程序员、审批员、管理员
仅查阅已发布版本	programs.read.released	操作工及以上
新建程序、上传版本、废弃	programs.write	程序员、管理员
提交审批	versions.submit	程序员、管理员

上述权限可按程序库范围授予，例如仅在试制程序库内授予程序员权限。角色与权限的完整定义见 6.1。

5.2 审批与放行

5.2.1 适用范围

本节规定版本从「待审批」转为「已发布」的判定规则与操作方法。适用于程序员、审批员与管理
员。

5.2.2 审批策略

审批策略按程序库配置，不设全局策略。同一车间可同时存在要求主管签字的量产程序库与允许 自审
自批的试制程序库。策略参数按表 5-6 的规定。

表 5-6 审批策略参数

参数	默认值	含义
审批人数	1	放行所需的不同审批人数量
禁止自审自批	启用	启用时，版本作者本人的批准不计入 票数
自动放行	停用	启用时，版本提交后直接发布，不进 入审批队列

典型配置组合按表 5-7 的规定选用。

表 5-7 典型审批策略组合

程序库类型	审批人数	禁止自审自批	自动放行	适用场合
量产程序库	1	启用	停用	常规配置
试制程序库	1	停用	启用	单人快速迭代
工装与对刀程序库	2	启用	停用	影响面较大的通用子 程序

注意

仅配备一名工程师的单位，应将该程序库设为自动放行，或停用「禁止自审自批」。不应在实际
只有一人操作的情况下配置多人审批流程，此类配置会使审计记录失去追溯意义。

5.2.3 审批队列

「审批」页列出当前用户待处理的全部版本，导航栏角标显示该队列长度。

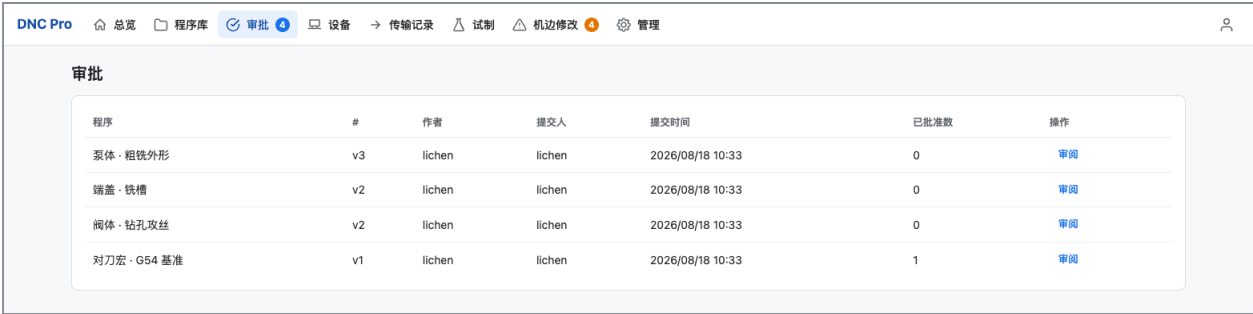


图 5-6 审批队列页面

队列各字段的含义按表 5-8 的规定。

表 5-8 审批队列字段

字段	说明
程序 / #	待审批版本所属的程序及其版本号
作者	创建该版本的人员
提交人	执行「提交审批」操作的人员，可与作者不同
已批准数	该版本已获得的有效票数。双人会签场合此处显示 1 表示尚差一票

5.2.4 评审操作

操作步骤：

- a) 在审批队列中单击「审阅」，打开评审弹窗；
- b) 选择「查看差异」（默认）核对与上一版本的并排差异，或选择「查看完整程序」核对本版全文；
- c) 在「意见」栏填写审批意见，该栏为必填项，批准与驳回均须填写；
- d) 单击「批准」或「驳回」。

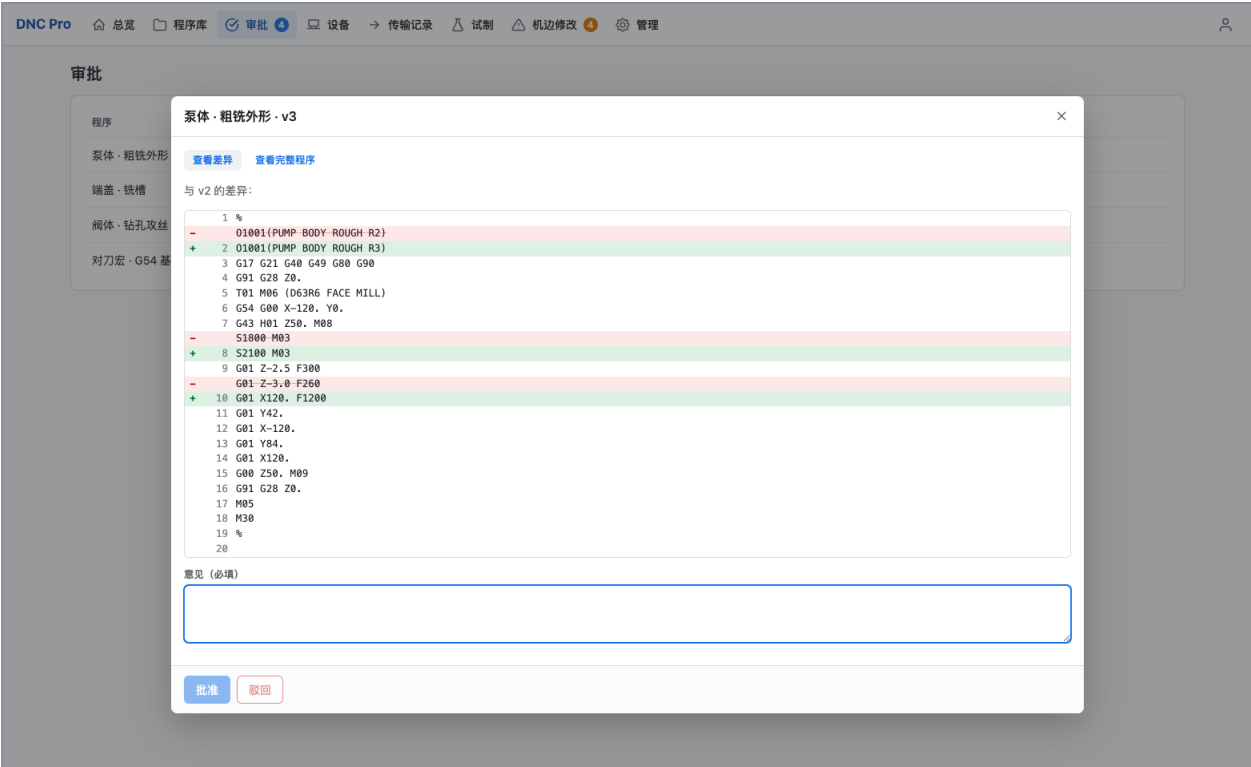


图 5-7 评审弹窗

说明

审批意见为必填项。意见内容构成后续追溯的直接依据，应记录判断理由与后续验证要求，例如首件检测项目、需关注的工艺参数。

5.2.5 放行判定

批准操作的处理规则如下：

- a) 有效票数达到「审批人数」时，版本状态转为「已发布」，进入下发候选列表，并触发 `version.released` Webhook；
- b) 有效票数未达到时，版本保持「待审批」，界面显示已获得的批准次数；
- c) 同一人员对同一版本的重复批准仅计一票；
- d) 在启用「禁止自审自批」的程序库内，作者本人执行批准将被拒绝。

驳回的处理规则：版本退回「草稿」状态，由作者修改后重新提交，版本号不变、内容为新的一版；驳回意见保留在审批记录中。

5.2.6 权限要求

表 5-9 审批相关权限

操作	所需权限	具备该权限的角色
批准、驳回版本	approvals.decide	审批员、管理员
提交审批	versions.submit	程序员、管理员

授权范围可设为全局，亦可限定至某个程序库。

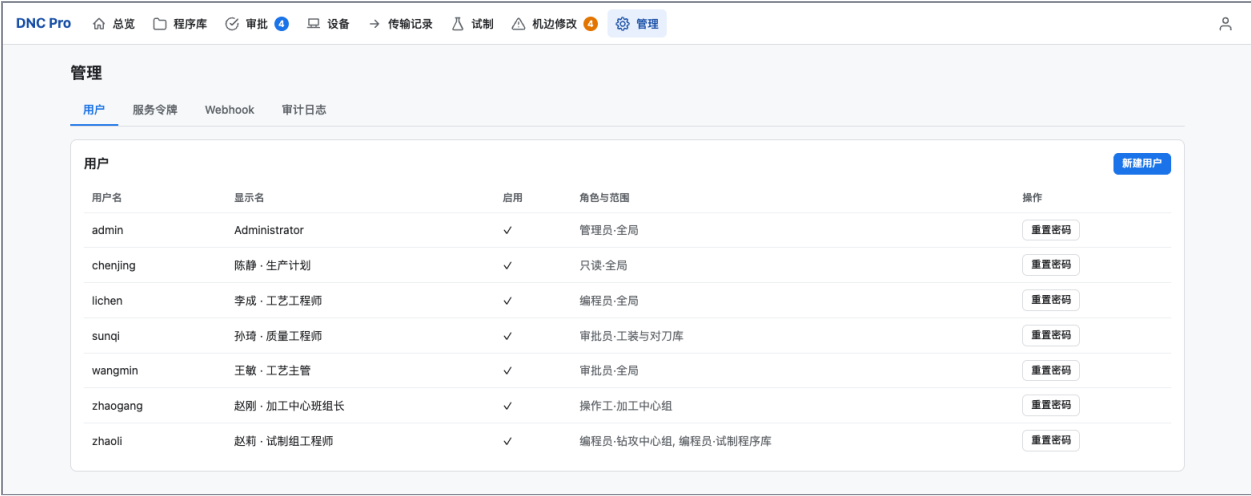


图 5-8 用户与授权页面

图 5-8 中，王敏为全局审批员，孙琦仅在「工装与对刀库」内具备审批员权限。该库的双人会签由二人共同完成。

5.2.7 相关说明

审批与内容外流。 审批人打开评审弹窗将读取程序正文，系统据此记录一条 `version.view` 审计记录。该记录属正常业务行为，审计查询方法见 5.9。

审批与试制的关系。 试制下发的对象仍为「已发布」版本，试制不构成绕过审批的通道。试制解决的是已批准版本尚未在具体机床上验证的问题，见 5.5。

5.3 机台分配与落地转换

5.3.1 适用范围

本节规定机台分配的建立方法与落地转换的配置规则。适用于程序员与管理员。分配是执行下发（5.4）的前置条件。

5.3.2 分配的定义

一条机台分配规定该程序下发至指定机台时的三项内容：

- a) 落地文件名；
- b) 落地目录；
- c) 内容的落地转换规则。

一个程序可建立多条分配，用于铺至多台机台；一台机台亦可承载多条分配，对应多个程序。

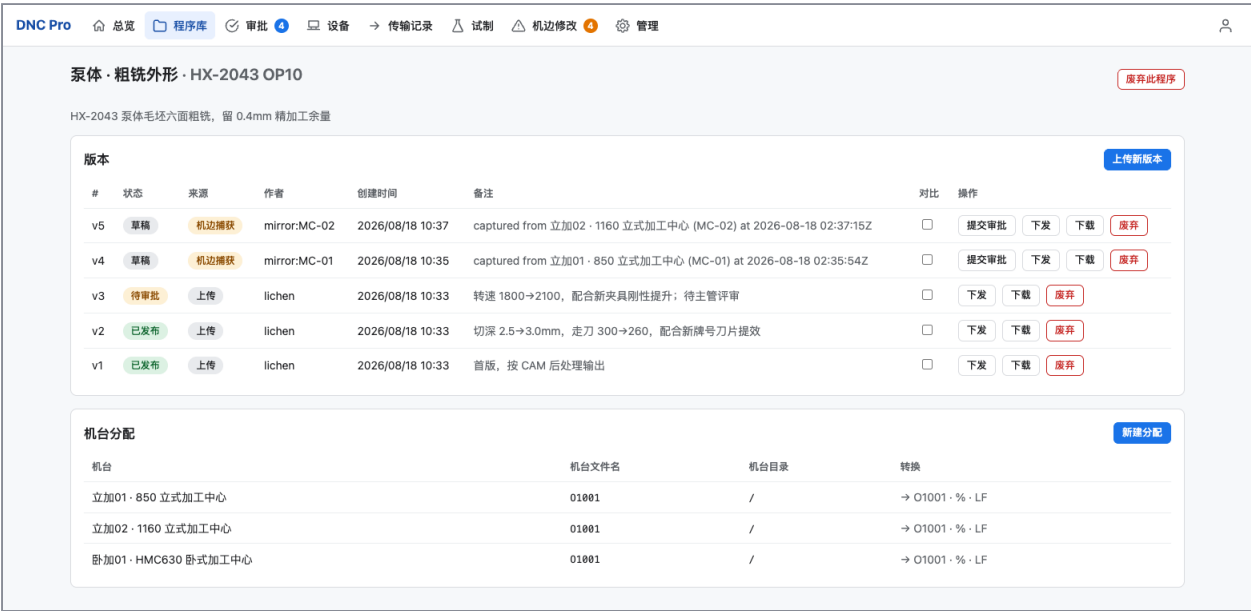


图 5-9 程序详情页面的机台分配列表

5.3.3 落地转换

落地转换按表 5-10 的规定配置。转换在发送前对内容执行，机床上落地的是转换后的字节；传输记录中的「转换后哈希」即为该字节序列的 SHA-256 值。

表 5-10 落地转换项

转换项	取值	适用条件
程序名改写	目标程序名，如 01001	FANUC 系统必设；其他系统按需
保证 % 包裹	启用 / 停用	启用后在内容首尾自动补 % 行
行结束符	LF / CRLF	目标控制系统对换行符敏感时设定
目标编码	编码名称	程序中含非 ASCII 注释时设定

5.3.4 FANUC 程序名规则

FANUC 控制器接收文件时忽略传入的文件名参数，程序名取自内容本身，即第一个换行符与第二个换行符之间的一行，见图 5-10。

```
%  
01001(PUMP BODY ROUGH)  
G17 G21 G40 G49 G80 G90  
...
```

← 第一行

← 控制器由此行取名：01001

图 5-10 FANUC 程序名的取值位置

尖括号形式 <PUMPROUGH> 同样有效。

警告

向 FANUC 机床建立分配时，「程序名改写」应设为与机台文件名一致的 O 号。若内容中的 O 号与机台文件名不一致且未设置改写，程序将以内容中的 O 号落地，后续向该机台文件名下发时将出现「目标为空」，且原有程序可能被覆盖于非预期的程序号下。

说明

FANUC 在列目录时会去除标准 O 号的前导零（00010 显示为 010），不同代次控制器的行为不一致。本系统在比对时对上述写法作归一化处理，因此机床屏幕显示的名称可能与配置值不完全相同，不影响一致性判定。其他厂商差异见 6.2。

5.3.5 落地目录

「机台目录」留空时使用该机台的文件根目录，根目录由网关的机床配置提供，例如 FANUC 为 //CNC_MEM/、西门子为 /nckfs、三菱为 PRG\USER\。

注意

部分控制系统不支持指定目录。在此类系统上填写的目录不生效，文件仍落至根目录。该行为属控制器限制，不属配置错误。

5.3.6 转换预览

分配建立后应执行一次转换预览，用于确认发出的内容正确。

操作步骤：

- a) 在分配上选择目标版本，执行「预览转换」；
- b) 核对输出的转换后完整文本，该文本即为将写入机床的字节；
- c) 记录输出的 SHA-256 值与字节数。

注意

预览得到的 SHA-256 值应与后续实际下发记录中的「转换后哈希」完全一致。两者不一致表明分配配置在两次操作之间被修改。排查下发内容异常时，应先执行转换预览确认发出内容，再检查机床侧。

5.3.7 批量分配与批次

批量下发时可一次勾选多条分配，系统据此生成一个批次，每台机台对应一条独立的下发记录。

各机台的下发事务相互独立，单台失败不影响也不回滚其他机台。批次仅作为查询用的分组。

5.3.8 文件名归一化

分配保存时记录一个归一化文件名，用于与机床列出的文件名匹配。FANUC 的 O 号零填充差异在该层被吸收，匹配规则示例按表 5-11 的规定。

表 5-11 文件名匹配示例

机床上的名称	分配中填写的名称	匹配结果	原因
00001	01	匹配	FANUC O 号的零填充差异被归一化吸收
PART.NC	part.nc	不匹配	非 FANUC 系统区分大小写

5.3.9 权限要求

表 5-12 分配相关权限

操作	所需权限	具备该权限的角色
建立、修改、删除机台分配	programs.write	程序员、管理员

授权范围可按程序库限定。角色与权限的完整定义见 6.1。

5.4 程序下发

5.4.1 适用范围

本节规定已发布版本或试制版本向数控机床下发的执行规则、结果判定与异常处置方法。适用于操作工、程序员与管理员。

5.4.2 前置条件

执行下发前应满足下列条件：

- a) 目标机台已建立机台分配，落地文件名、目录与转换规则均已确认（见 5.3）；
- b) 待下发版本处于「已发布」状态，或为经批准的试制版本（见 5.5）；
- c) 操作人员具备 `deployments.send.released` 或 `deployments.send.proveout` 权限，且授权范围覆盖目标机组；
- d) 目标机台所属网关在线。

警告

下发将删除机床上的目标文件后重新写入。执行前应确认目标机床未处于加工状态，且目标程序未被机床调用。对正在运行的程序执行下发可能造成加工中断或工件报废。

5.4.3 事务模型

向机床写入程序文件包含删除、写入、确认三个动作。任一动作中断将使机床停留在内容不确定的中间状态。

本系统将上述动作封装为单一事务，执行结果仅有两种：机床上为经校验的新版本，或机床上保持原有程序。不存在第三种结果。

5.4.4 执行阶段

下发按图 5-11 所示的六个阶段顺序执行，各阶段的动作与失败处置按表 5-13 的规定。



图 5-11 下发事务的阶段流程

表 5-13 下发事务阶段与失败处置

阶段	动作	失败时的处置
① 预检	校验机床可达性、程序号未被锁定、分配有效	机床未被改动，无需回滚
② 快照	读回机床上现有内容并存为快照	机床未被改动，无需回滚
③ 删除	删除目标文件	明确未删除时无需回滚；结果不明时执行回滚
④ 发送	写入转换后的内容	执行回滚
⑤ 回读	读回刚写入的内容	执行回滚
⑥ 校验	归一化后逐字节比对回读内容与发送内容	执行回滚，并将该文件标记为异常

下发结果仅在第 ⑥ 阶段通过时判定为「成功（已校验）」。发送完成或回读完成均不作为成功判据。

说明

快照阶段发现机床上尚不存在该文件时，事务记录「目标为空」。此种情形下的回滚动作为 删除可能写入的不完整文件，而非恢复不存在的旧版本。

5.4.5 回滚结果

回滚结果按表 5-14 的规定取值。

表 5-14 回滚结果

回滚结果	含义	机床上的内容
无需回滚	失败发生在机床被改动之前	原有程序，未改动
已回滚	快照已成功写回并经回读确认	原有程序
回滚失败	快照写回失败	不确定

警告

回滚结果为「回滚失败」的文件处于内容未知状态。应在恢复生产前由具备机床操作资质的人员到机边核对实际程序内容，确认无误后方可继续加工，不得依据系统显示的版本号直接投产。

回滚失败的记录在设备页与机边操作台上持续显示，直至下一次成功的校验将其清除。

5.4.6 传输记录

DNC Pro

总览

程序库

审批

设备

传输记录

试制

机边修改

管理

刷新

机台全部机台

状态全部状态

共 16 条, 0 进行中, 1 失败

机台	文件	状态	失败阶段	回滚	试制	排队时间	完成时间
立加02 · 1160 立式加工中心	09002	成功 (已校验)				2026/08/18 10:48:44	2026/08/18 10:48:44
钻攻01 · S700X1	01180	成功 (已校验)				2026/08/18 10:37:14	2026/08/18 10:37:14
精雕01 · JD-400	07002	成功 (已校验)			试制	2026/08/18 10:35:45	2026/08/18 10:35:45
五轴01 · UMC750	SJ9001_0P10.MPF	成功 (已校验)			试制	2026/08/18 10:35:44	2026/08/18 10:35:44
车铣复合01 · CTX310	06001	失败 send failed: Network fault.	发送	已回滚		2026/08/18 10:35:44	2026/08/18 10:35:44
高速铣01 · HSM600	DG3320_0P20.MPF	成功 (已校验)				2026/08/18 10:35:35	2026/08/18 10:35:35
数车01 · CK6150	04001	成功 (已校验)				2026/08/18 10:35:34	2026/08/18 10:35:34
钻攻02 · TC-S2D	01180	成功 (已校验)				2026/08/18 10:35:34	2026/08/18 10:35:34
钻攻01 · S700X1	01180	成功 (已校验)				2026/08/18 10:35:34	2026/08/18 10:35:34
立加01 · 850 立式加工中心	01002	成功 (已校验)				2026/08/18 10:35:33	2026/08/18 10:35:33
卧加01 · HMC630 卧式加工中心	09002	成功 (已校验)				2026/08/18 10:35:33	2026/08/18 10:35:33
立加02 · 1160 立式加工中心	09002	成功 (已校验)				2026/08/18 10:35:33	2026/08/18 10:35:33
立加01 · 850 立式加工中心	09002	成功 (已校验)				2026/08/18 10:35:33	2026/08/18 10:35:33
卧加01 · HMC630 卧式加工中心	01001	成功 (已校验)				2026/08/18 10:35:32	2026/08/18 10:35:32
立加02 · 1160 立式加工中心	01001	成功 (已校验)				2026/08/18 10:35:32	2026/08/18 10:35:32
立加01 · 850 立式加工中心	01001	成功 (已校验)				2026/08/18 10:35:32	2026/08/18 10:35:33

图 5-12 传输记录页面

传输记录各字段的含义按表 5-15 的规定。

表 5-15 传输记录字段

字段	说明
机台 / 文件	目标机台及落地文件名
状态	排队中 / 成功（已校验） / 失败
失败阶段	失败发生在表 5-13 六个阶段中的哪一个
回滚	无需回滚 / 已回滚 / 回滚失败
试制	本次下发是否为试制（见 5.5）
排队时间 / 完成时间	任务的入队时刻与结束时刻

页面顶部可按机台与状态筛选，右上角显示「共 N 条，M 进行中，K 失败」。总览页的「24 小时内失败传输」链接至本页的失败筛选视图。

5.4.7 异常处置

下发失败后按下列顺序处置：

- a) 查看失败阶段。失败发生在预检或快照阶段时，机床未被改动，可直接排查网络与机床状态；
- b) 查看回滚结果。结果为「已回滚」时，机床上为原有版本，生产可继续；结果为「回滚失败」时，按 5.4.5 的警告执行机边人工核对；
- c) 查看失败详情。详情信息（例如 `send failed: Network fault.`）直接来自网关；
- d) 排除故障后重新下发。下发操作具备幂等性，可直接重试。

常见失败原因与处理措施见 7.3。

5.4.8 归一化比对

第 ⑥ 阶段的比对不是简单的字节相等比较。不同控制器在存取文件时会引入无害变换，包括：

- a) 行结束符被统一；
- b) FANUC 的 O 号前导零被去除；
- c) 末尾空行被增删。

本系统按目标机床的厂商画像执行归一化后再比对，避免将控制器的正常行为判定为内容不一致。真实的内容差异（即使仅相差一个字符）均能被检出。厂商差异见 6.2。

5.4.9 并发规则

- a) 同一台机台在同一时刻仅执行一个传输任务；
- b) 滚动镜像向真实传输让路，每一次网关调用之间均执行让路检查；
- c) 滚动镜像跳过机床当前正在运行的程序。

因此后台备份不会导致下发变慢或被中断。滚动镜像的规则见 5.6。

5.4.10 权限要求

表 5-16 下发相关权限

操作	所需权限	具备该权限的角色
下发已发布版本	deployments.send.released	操作工、程序员、管理员
下发试制版本	deployments.send.proveout	程序员、管理员

授权范围可按机组限定，例如操作工仅可对本机组的机台执行下发。角色与权限的完整定义见 6.1。

5.5 试制

5.5.1 适用范围

本节规定试制（试切）下发的执行规则与到期处置方法。适用于程序员与管理员。

试制用于已批准的版本在具体机床、具体毛坯与夹具条件下尚未切实验证的场合。

5.5.2 试制解决的问题

未纳入管理的试制操作存在下列风险：

- a) 试制结束后未撤回，次日班次将其当作正式程序批量加工；
- b) 试制时覆盖了机床上原有的受控版本，试制结束后无法恢复；
- c) 其他人员无法从机床上区分试制程序与正式程序。

5.5.3 前置条件

- a) 待下发版本处于「已发布」状态；
- b) 目标机台已建立机台分配（见 5.3）；
- c) 操作人员具备 `deployments.send.proveout` 权限；
- d) 目标机台所属机组未启用「禁止试制」。

5.5.4 操作步骤

- a) 在下发操作中勾选「试制」，并设定试制时长（单位：小时）；
- b) 执行下发。下发过程与规则同 5.4，无差别；
- c) 在试制页面监视剩余时间；
- d) 到期后按 5.5.6 执行转正或撤回。

试制下发后的系统行为：

- a) 该次下发在全部界面上带「试制中」徽标；
- b) 系统记录到期时刻，界面显示剩余时间倒计时；
- c) 到期后状态转为「已过期」并继续显示，等待人工处置。

警告

系统不因试制到期而自动改动机床。到期仅将标记由「试制中」改为「已过期」。试制版本未经切实验证确认，不得用于批量生产。



图 5-13 试制页面

试制页面默认仅显示进行中的试制，取消该筛选可查阅历史记录。

5.5.5 试制处置

到期处置方式按表 5-17 的规定，二者必选其一。

表 5-17 试制处置方式

处置方式	系统动作	机床上的内容
转正	该版本成为该机台上的正式受控内容，解除试制标记	保持不变，不发生传输
撤回	将上一版受控内容推回机床，试制记录标记为已撤回	恢复为上一版受控内容

说明

撤回是一次完整的事务式下发，同样执行快照、回读与校验，同样记入传输记录，可按 5.4 的规则查阅与处置。

5.5.6 机组级禁止试制

对不应出现试制程序的机床（量产节拍机、无人值守夜班机、安全等级较高的工位），应在机组级别停用「允许试制」。

操作步骤：进入「设备 → 机组」，停用该机组的「允许试制」开关。

停用后，该机组内全部机台的试制下发请求均被系统拒绝。

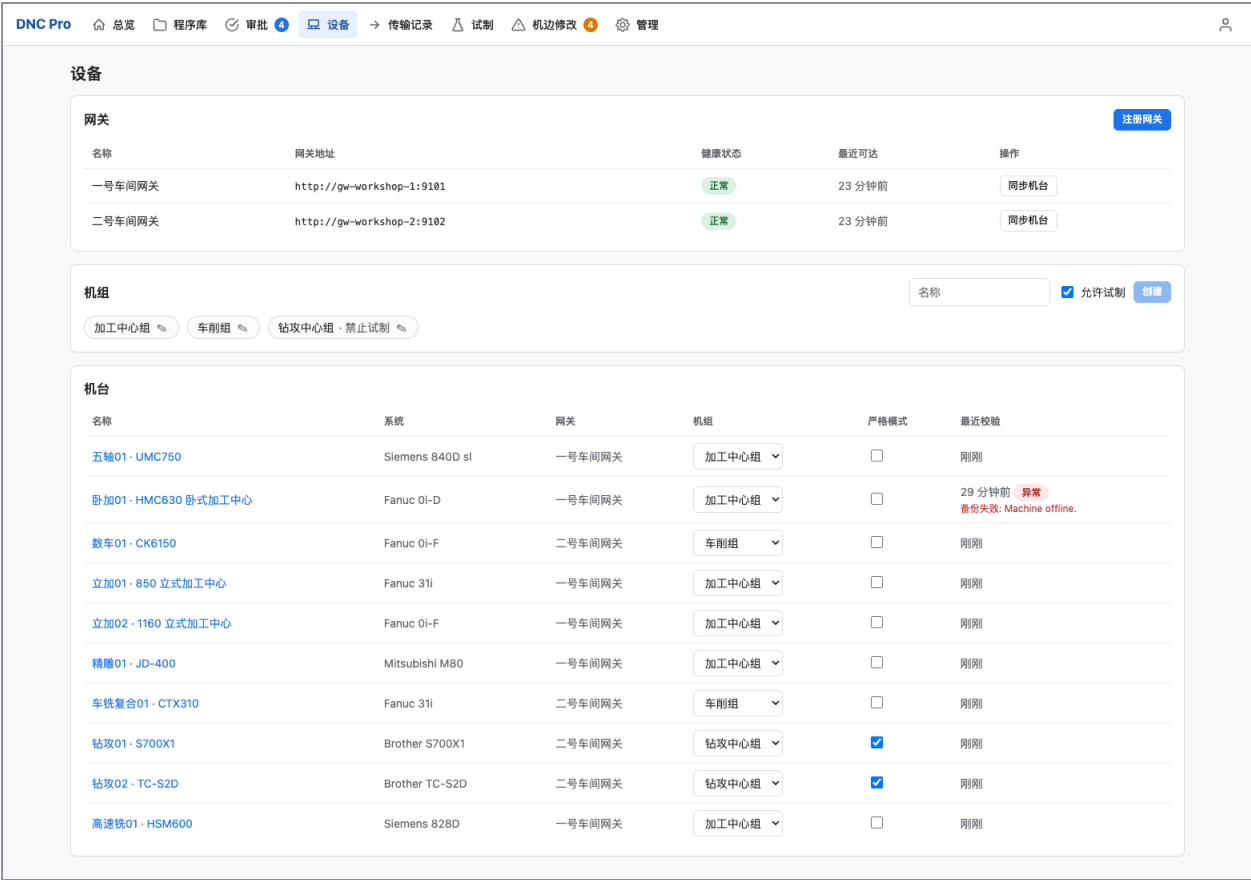


图 5-14 设备页面的机组策略

图 5-14 中「钻攻中心组」已配置为禁止试制。该策略由系统强制执行，不依赖人员记忆。

5.5.7 试制期间的机边修改

试制期间调整加工参数属预期行为。因此进行中的试制（含已过期未处置的试制）将抑制该文件的机边修改捕获，不在机边修改队列中重复产生记录。

改动内容仍由滚动镜像完整备份，可随时取回，见 5.6。试制转正时，可基于机床上的最终内容重新执行上传或采纳。

5.5.8 与审批的关系

试制下发的对象为「已发布」版本，试制不构成绕过审批的通道， 而是审批之后、正式量产之前的一道验证。

注意

需要在版本获批前先行试制的场合，应为该类程序单独配置自动放行的试制程序库（见 5.2），不应通过其他方式绕过审批。

5.5.9 权限要求

表 5-18 试制相关权限

操作	所需权限	具备该权限的角色
试制下发	deployments.send.proveout	程序员、管理员
试制转正、撤回	deployments.send.proveout	程序员、管理员

操作工不具备试制下发权限，仅可下发已发布的正式版本。该限制为设计约定：判定某一版本可否用于试制属工艺决策，不属操作决策。

5.6 滚动镜像与快照

5.6.1 适用范围

本节规定滚动镜像的运行规则、快照的产生与还原方法，以及未受管文件的处理规则。适用于编程
员、设备管理人员与管理员。

5.6.2 功能说明

滚动镜像是持续运行的后台循环。它轮转扫描全部机台，逐台读回机床上的每一个文件，存为按内容
寻址的快照。

保护范围为机床上的全部文件，不限于受管程序，包括历年积累的、未纳入任何管理体系的 机床本地
程序。

5.6.3 执行规则

滚动镜像的执行规则按表 5-19 的规定。设计前提为：镜像的优先级始终低于生产。

表 5-19 滚动镜像执行规则

规则	说明	默认值
单网关并发限制	每台网关同一时刻仅扫描一台机床	—
请求节流	相邻网关请求之间的间隔	250 ms
空闲休眠	完成一轮后休眠再重新开始	5 s
传输让路	每一次网关调用前检查是否存在待执行的传输任务，有则让路	—
跳过运行中程序	不读取机床当前正在运行的文件	—
校验时间更新条件	仅在完整扫描完成时更新「最近校验」	—

说明

「最近校验」仅在一轮扫描完整完成时更新。若某机台的「最近校验」停留在两小时前，即表示
该机台确已两小时未完成成功备份，而非部分文件失败。

5.6.4 镜像异常的识别

镜像失败记录在对应机台上，可在设备页、机台详情页与机边操作台上查阅，总览页的「镜像异常机台」给出计数。

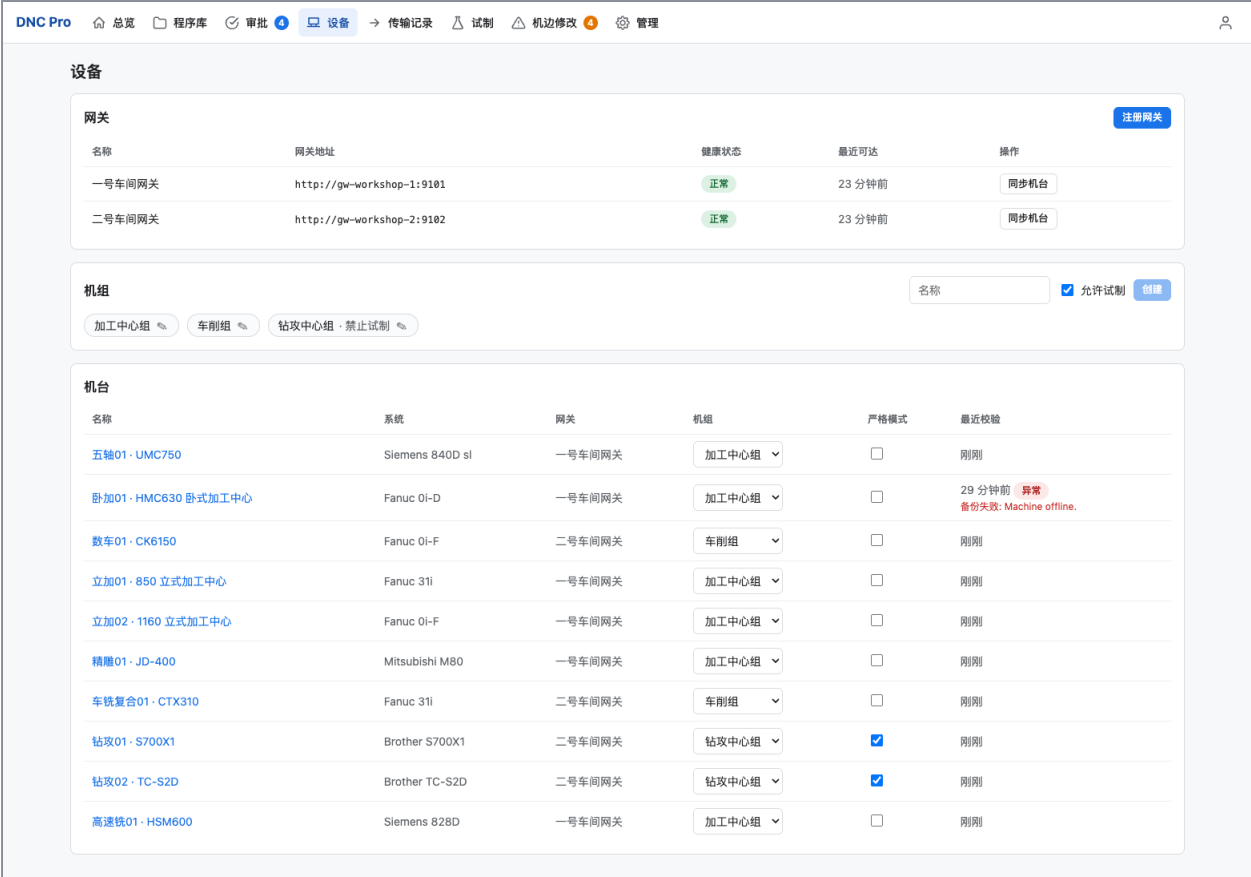


图 5-15 设备页面的机台备份状态

图 5-15 中，卧加 01 的备份失败原因直接显示在行内，无需查阅服务器日志。

注意

镜像异常应按告警处理。持续处于镜像异常的机台不具备可用的备份，其机边修改也不会被检出。

5.6.5 立即检查

「立即检查」将指定机台插入镜像队列最前端，用于需要立即确认机床内容的场合。

操作位置：

- a) 控制台：机台详情页右上角的「立即检查」；

b) 机边操作台：机台页面的「我改了程序，立即检查」按钮。



图 5-16 机边操作台的立即检查入口

5.6.6 快照与还原

每个文件的每一代内容均存为快照，快照来源按表 5-20 的规定。

表 5-20 快照来源

来源	产生时机
下发前快照	事务式下发的第 ② 阶段（见 5.4）
回读快照	下发校验通过后，存下回读到的内容
镜像快照	滚动镜像检出内容变化时

还原操作步骤：

- a) 进入机台详情页，在目标文件行单击「快照」；
- b) 在历史列表选定目标代次；
- c) 单击「还原」。

注意

还原经由与下发相同的事务式管线执行（快照 → 删除 → 发送 → 回读 → 校验），执行前应确认机床未处于加工状态，处置规则同 5.4。

机床控制器数据被清空后的恢复流程：

- a) 进入机台详情页，逐个文件执行快照还原；
- b) 受管文件亦可直接重新下发最新的已发布版本。

本系统自身的数据同时丢失时，应先自备份恢复本系统的数据，再执行上述步骤， 见 6.4。

5.6.7 未受管文件

机床上不属于任何机台分配的文件为未受管文件。受管文件与未受管文件的处理差异 按表 5-21 的规定。



图 5-17 机台详情页面的文件列表

表 5-21 受管文件与未受管文件的处理差异

处理项	受管文件	未受管文件
镜像备份与历史快照	✓	✓
快照还原	✓	✓
内容一致性检查	✓	✗
机边修改捕获与处置	✓	✗

未受管文件不被检查也不被纠正，其改动不产生机边修改记录。该规则适用于对刀宏、 暖机程序、临时工装程序等无需走审批流程但不得丢失的内容。

严格模式为机台级开关，启用后在文件列表中高亮标出未受管文件， 仅作提示，不阻断任何操作。 适用于不允许出现计划外程序的机台。

5.6.8 采纳未受管文件

采纳将未受管文件收入指定程序库，纳入受控管理。

操作步骤：

- a) 单个文件：在文件行单击「采纳」；整台机台：在右上角选定目标程序库后单击「全部采纳」；
- b) 填写程序名称、零件号与工序；
- c) 确认执行。

采纳后系统执行下列动作：

- a) 在目标程序库中建立一个程序；
- b) 以机床上的当前内容建立 v1，来源标记为「采纳」；
- c) 自动建立一条指向该机台该文件名的机台分配。

注意

采纳建立的 v1 是机床上的当前内容，其工艺正确性未经确认。应在采纳后先行人工审阅，再决定是否作为基线发布。

5.6.9 存储占用

快照按内容哈希去重。镜像扫描的绝大多数结果为内容未变，不产生新的存储占用，实际占用仅来自发生过的每一次内容变更。

以 30 台机床、每台 40 个程序的规模估算，程序内容总量通常为数十兆字节量级，快照历史的累计占用远低于单张图纸扫描件。

5.6.10 关闭滚动镜像

滚动镜像默认启用。仅在网关侧资源极度紧张等个别场合可关闭，关闭在系统配置中进行，控制台上不提供该开关。

警告

关闭滚动镜像即放弃全部备份能力与机边修改检测能力。关闭后下发仍可执行，但机床上的实际内容是否与受控版本一致将无法判定，控制器数据丢失后亦无快照可供还原。

5.7 机边修改的处置

5.7.1 适用范围

本节规定受管文件在机床侧被改动后的系统行为与人工处置方法。适用于程序员与管理员。

5.7.2 处置原则

操作工在控制面板上调整进给、转速与切深，多数情况下是基于现场判断的正确改动。需要管理的不是改动行为本身，而是改动未被记录、未被评审的状态。

本系统的处置原则为：捕获改动、呈现差异、由工程师决定。

注意

系统不会自动还原机床上的内容。无论采纳或拒绝，机床内容的改动均须由人员显式发起。

5.7.3 捕获规则

滚动镜像检出某受管文件的内容与本系统期望内容不一致时，执行下列动作：

- a) 将机床上的当前内容存为一个新版本，来源标记为「机边捕获」，状态为「草稿」；
- b) 建立一条机边修改记录，状态为「待处置」；
- c) 触发 `drift.captured` Webhook；
- d) 在导航栏角标、总览页卡片与机边修改队列上计入。

期望内容按下列规则解析：

- a) 若存在一条未处置的机边修改，则期望内容为该次捕获的内容。此后的继续改动仅更新同一条记录，不产生新记录；
- b) 否则取下列三者中最新的一项：上一次被采纳的机边修改、上一次成功下发的回读内容、采纳基线。

未受管文件不参与上述逻辑，其改动被备份但不被检查，见 5.6。

5.7.4 处置操作

操作步骤：

- a) 进入「机边修改」页，在队列中选定待处置记录；
- b) 核对捕获版本与受控版本的差异；
- c) 填写处置意见，该栏为必填项；
- d) 选择「采纳修改」或「拒绝修改」；拒绝时按需勾选「并将已发布版本推回机台」。

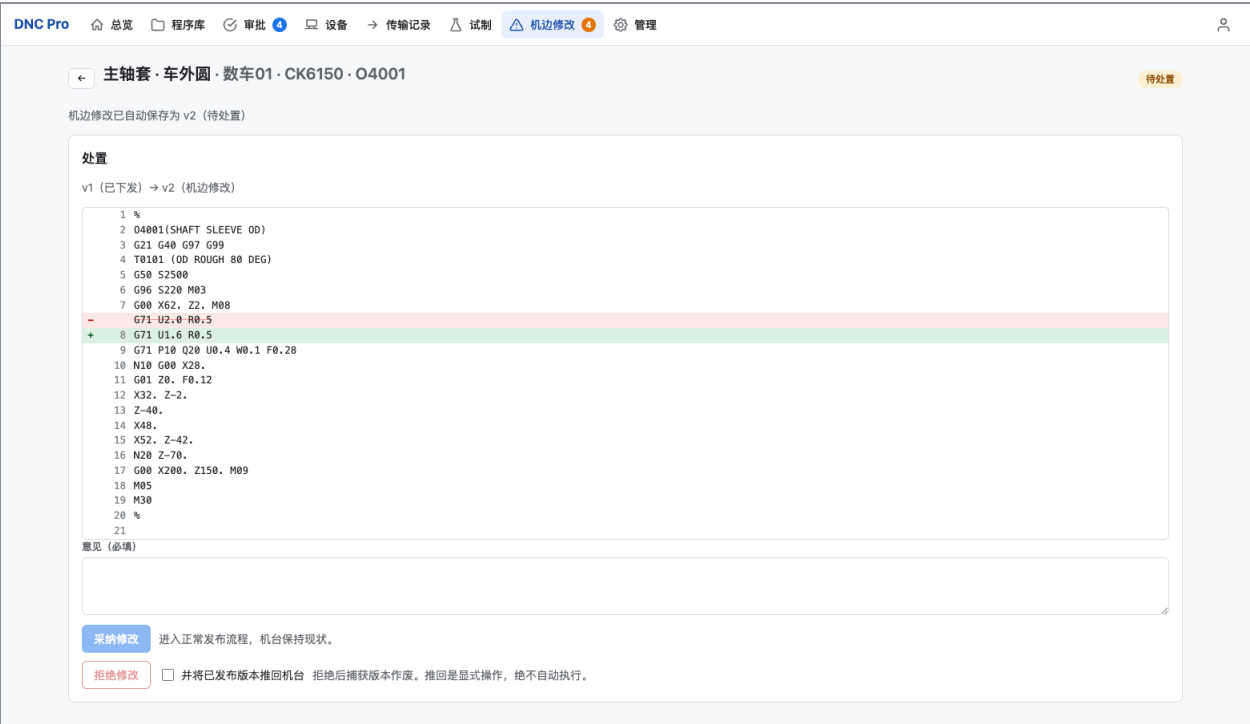


图 5-18 机边修改处置页面

处置方式的系统动作按表 5-22 的规定。

表 5-22 机边修改处置方式

处置方式	系统动作	机床上的内容
采纳修改	捕获版本进入正常发布流程（提交审批 → 放行）	保持现状，不发生传输
拒绝修改	捕获版本作废	保持现状；勾选「推回机台」时恢复为已发布版本

5.7.4.1 采纳后的流转

采纳后的完整流转见图 5-19。

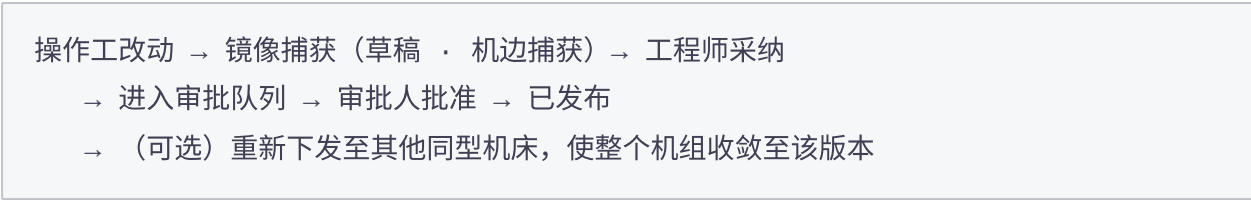


图 5-19 机边修改的采纳流转

该流转将单台机床上的一次现场改动转为整个机组的一次受控工艺变更，全程留有审批与审计记录。

5.7.4.2 拒绝并推回

勾选「推回机台」后，系统对该机台执行一次完整的事务式下发，将当前已发布版本写回机床。该次传输记入传输记录，其规则与普通下发一致，见 5.4。

警告

推回将覆盖机床上的当前内容。执行前应确认机床未处于加工状态，且已确认被覆盖的改动无需保留。改动内容仍保存在捕获版本与镜像快照中，可供事后取回。

不勾选「推回机台」时仅关闭该条记录，机床上保持被改动后的内容。适用于改动已知悉、暂按现状运行、正式版本另行安排的情形。

5.7.5 试制期间的抑制规则

进行中的试制（含已过期未处置的试制）抑制该文件的机边修改捕获。试制期间调整参数属预期行为，不逐次产生记录。改动内容仍由滚动镜像完整备份，见 5.5。

5.7.6 队列说明

DNC Pro

总览

程序库

审批 4

设备

→

传输记录

试制

机边修改 4

管理

机边修改

☒ 仅显示待处理

机台	程序	文件	捕获版本	发现时间	状态	操作
立加01 · 850 立式加工中心	泵体 · 精铣密封面	01002	v2	17 分钟前	待处置	审阅
立加02 · 1160 立式加工中心	泵体 · 粗铣外形	01001	v5	28 分钟前	待处置	审阅
高速铣01 · HSM600	端盖 · 铣槽	DG3320_OP20.MPF	v3	29 分钟前	待处置	审阅
数车01 · CK6150	主轴套 · 车外圆	04001	v2	30 分钟前	待处置	审阅

图 5-20 机边修改队列

队列每条记录给出机台、文件名、对应程序与检测时间。总览页的「待处理机边修改」卡片列出最近若干条并提供跳转入口。

说明

机边修改队列长期为空通常有两种原因：程序已充分成熟，或操作工因改动会被覆盖而不再反馈现场经验。后者较为常见。队列中稳定存在少量记录并被及时处置，表明现场反馈通道处于有效状态。

5.7.7 权限要求

表 5-23 机边修改相关权限

操作	所需权限	具备该权限的角色
采纳、拒绝机边修改	drift.disposition	程序员、管理员

授权范围可按机组或程序库限定。审批员与操作工不具备该权限：机边修改的处置属工艺决策。角色与权限的完整定义见 6.1。

5.8 机边操作台

5.8.1 适用范围

本节规定机边操作台的使用方法。适用于操作工。

机边操作台运行于车间工位的触摸屏或平板设备，访问地址为 `http://<主机>:8030/shopfloor/`。

其设计约束为：

- a) 仅显示当前用户授权范围内的机台；
- b) 仅显示该机台应当运行的程序；
- c) 以状态标识直接给出机床上的内容是否为最新受控版本。

5.8.2 登录

操作步骤：使用操作工本人的账号登录。

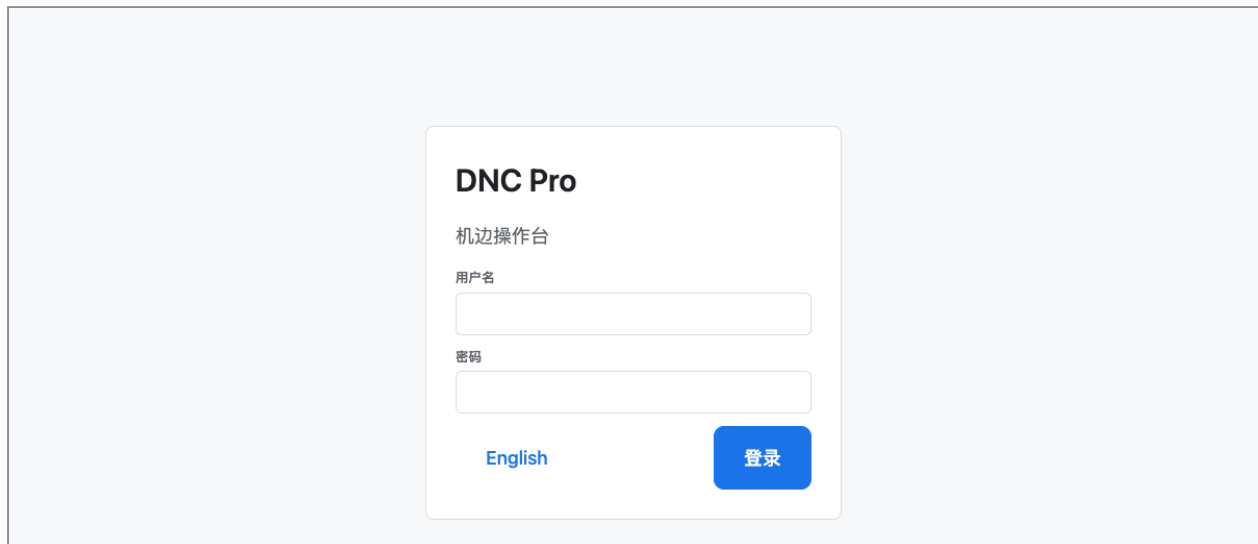


图 5-21 机边操作台登录界面

注意

一台触摸屏可供整个班组共用，但每人应使用本人账号登录。审计记录须可追溯至具体人员。

5.8.3 机台列表



图 5-22 机边操作台的机台列表

列表仅显示当前用户授权机组内的机台。图 5-22 中该用户的授权范围为「加工中心组」， 故仅显示该组的 6 台机台。

每张卡片给出机床名称、控制系统型号、最近检查时间与程序数量。 存在镜像异常的机台显示「备份异常」标记，处理方法见 5.6。

5.8.4 机台页面



图 5-23 机边操作台的机台页面

每个程序对应一张卡片，给出程序名、零件号与工序、机床上的文件名、当前受控版本号， 以及「发送到机床」按钮。单击该按钮后需再次确认。

程序状态标识及其处理要求按表 5-24 的规定。

表 5-24 机边操作台的程序状态

状态标识	含义	应采取的操作
机床上已是最新版本	机床内容与受控版本一致	可开始加工
机床上不是最新版本	机床上为旧版本	执行「发送到机床」
尚未发送到此机床	该机台尚无此程序	执行「发送到机床」
机床上的程序被改过，等待编程员处理	存在待处置的机边修改（见 5.7）	联系工艺人员，不得自行覆盖
无已发布版本	该程序尚无可用的已发布版本	联系工艺人员

页面顶部另给出两项整机提示：最近检查时间，以及「N 个文件状态异常，请联系编程员」（对应回滚失败等情形，见 5.4）。

警告

「发送到机床」执行一次标准的事务式下发，与控制台上的下发为同一条管线，同样执行快照、回读与校验。执行前应确认机床未处于加工状态，见 5.4。

5.8.5 立即检查

页面顶部的「我改了程序，立即检查」按钮将该机台插入滚动镜像队列最前端。

在机床上完成参数调整后应主动执行本操作。改动将在数秒内被捕获为机边修改记录，进入工程师的处置队列，见 5.7。未执行本操作时，改动须等待下一轮镜像扫描才被检出，其间存在被下发覆盖的可能。

说明

本操作宜在班前会上向操作人员说明：在机床上调整的参数经此按钮上报后，工艺人员可查阅并可能将其采纳为正式版本。

5.8.6 操作工的权利边界

表 5-25 操作工的权利边界

操作项	允许	说明
查阅授权机组内的机台	✓	其他机组的机台不可见
查阅已发布版本	✓	草稿与待审批版本不可见

操作项	允许	说明
下发已发布版本	✓	—
请求立即检查	✓	—
下发试制版本	✗	属工艺决策，见 5.5
处置机边修改	✗	属工艺决策，见 5.7
查看、下载程序正文	✗	操作工不具备 <code>programs.content.view</code>

操作工可将正确的程序下发至机床，但不能取出程序内容。角色与权限的完整定义见 6.1。

5.8.7 语言切换

界面右上角可在简体中文与 English 之间切换，所选语言记录在本台设备上，无需为外籍或跨厂调机人员另行配置。

5.8.8 使用环境要求

- a) 触摸屏宜使用 Chrome 或 Edge 的全屏模式 (kiosk mode)，主页设为 `/shopfloor/`；
- b) 每名操作人员应使用本人账号登录；
- c) 屏幕分辨率不低于 1280×800。界面自适应，低于该分辨率仍可使用，但信息密度下降。

5.9 系统管理与审计

5.9.1 适用范围

本节规定「管理」页四个标签页的使用方法。全部操作均需 admin 权限，适用于管理员。

5.9.2 用户与授权

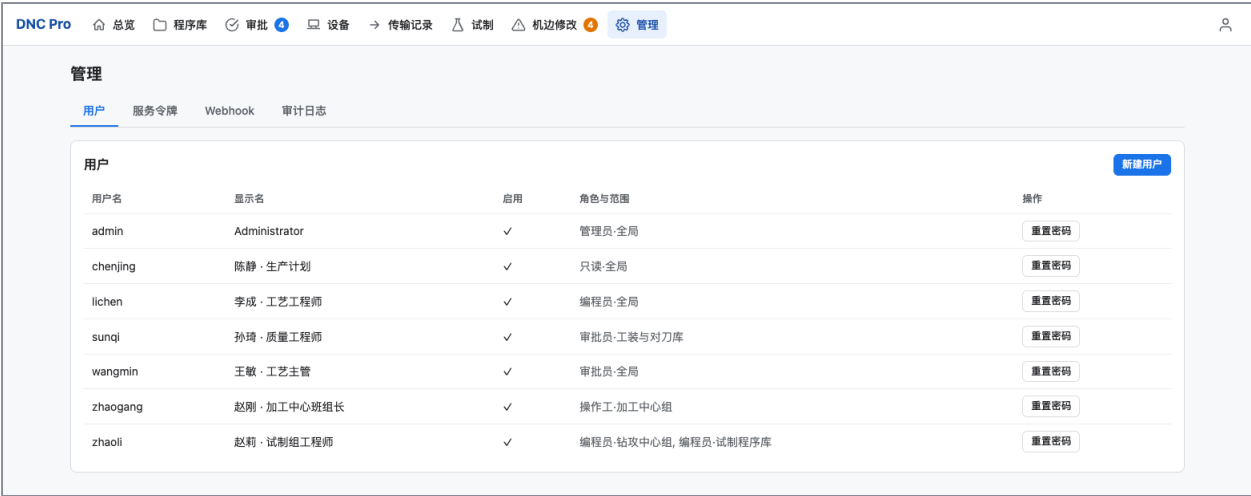


图 5-24 用户管理页面

新建用户时须为其指定一组授权，每条授权由「角色 × 范围」构成。范围类型按表 5-26 的规定。

表 5-26 授权范围类型

范围类型	作用域
全局	整个系统
机组	仅该机组内的机台（见 4.2）
程序库	仅该程序库内的程序（见 5.1）

一名用户可持有多条授权。例如演示环境中的赵莉持有「编程员·钻攻中心组」与「编程员·试制程序库」两条授权，因而可在试制库内编写程序、向钻攻中心组下发，但无权访问量产库与加工中心组。

角色能力的完整定义见 6.1。

密码管理：管理员可执行重置密码；用户在右上角账户菜单中自行修改密码，修改时须提供当前密码。

5.9.2.1 认证方式

- a) 本地账号：密码以哈希形式存储，可在完全断网条件下使用，具备登录失败锁定机制；
- b) OIDC 单点登录（可选）：对接企业身份源，授权关系仍在本系统侧管理。

说明

两种认证方式可并存。建议保留至少一个本地管理员账号，以便在企业身份源不可用时仍能登录系统。

5.9.3 服务令牌

机器对机器的集成（MES、CAM 后处理、看板等）应使用服务令牌，不应使用人员账号。



图 5-25 服务令牌页面

令牌格式为 `dncp_<id>_<secret>`，调用时置于 `Authorization: Bearer dncp_...` 请求头。

注意

令牌明文仅在创建时显示一次，系统仅存储其哈希值。应在创建时立即记录并按本单位密钥管理制度保管。遗失后只能吊销重建。

令牌属性按表 5-27 的规定配置。

表 5-27 服务令牌属性

属性	说明
角色与范围	适用与人员账号相同的权限规则，不存在越权令牌
可代理身份	允许令牌通过 <code>X-On-Behalf-Of</code> 请求头声明本次操作的实际发起人
高危需操作人	启用后，下发、删除等高危操作必须携带操作人，否则拒绝执行

属性	说明
有效期	到期自动失效，亦可随时吊销

代理身份用于审计追溯：由 MES 自动触发的下发，审计日志同时记录主体（MES 令牌） 与操作人（提交工单的人员）。

5.9.4 Webhook 订阅

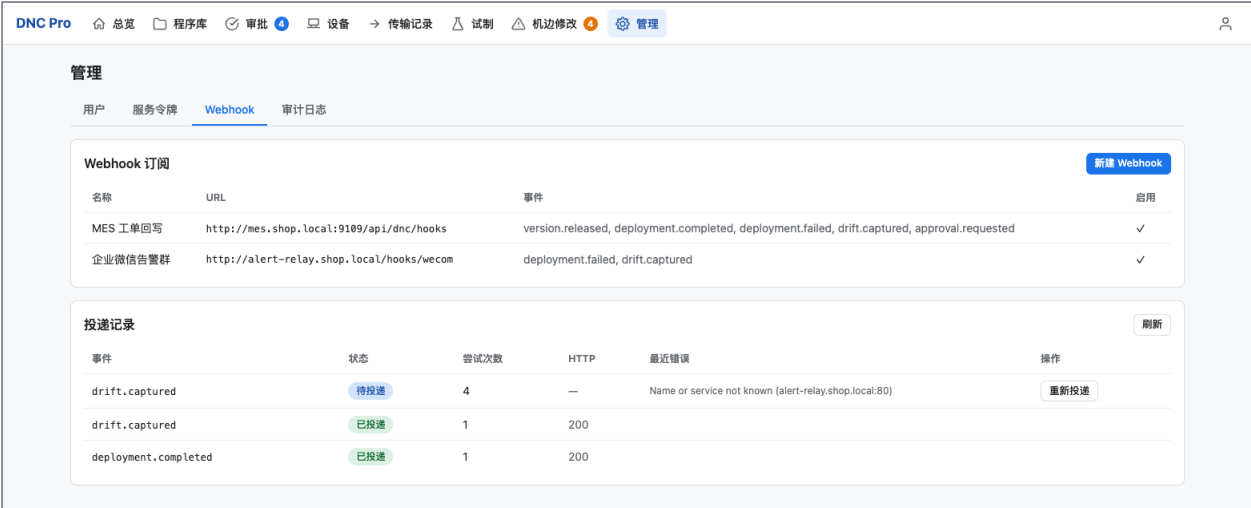


图 5-26 Webhook 订阅页面

可订阅的事件按表 5-28 的规定。

表 5-28 可订阅的 Webhook 事件

事件	触发时机
version.released	版本审批通过并放行
deployment.completed	下发通过回读校验
deployment.failed	下发失败，负载中含失败阶段与回滚结果
drift.captured	捕获到一条机边修改
approval.requested	有版本提交审批

注意

每个订阅具备独立密钥，投递请求携带签名。接收端应先校验签名再处理负载， 不应直接信任未校验的请求。

「投递记录」表给出每一次投递的事件、状态、尝试次数、HTTP 响应码与最近一次错误信息。投递失败自动重试，亦可手动执行重新投递。

图 5-26 中，`alert-relay.shop.local` 不可达，重试 3 次后状态仍为「待投递」，错误原因显示在行内，可据此排查集成故障。

5.9.5 审计日志

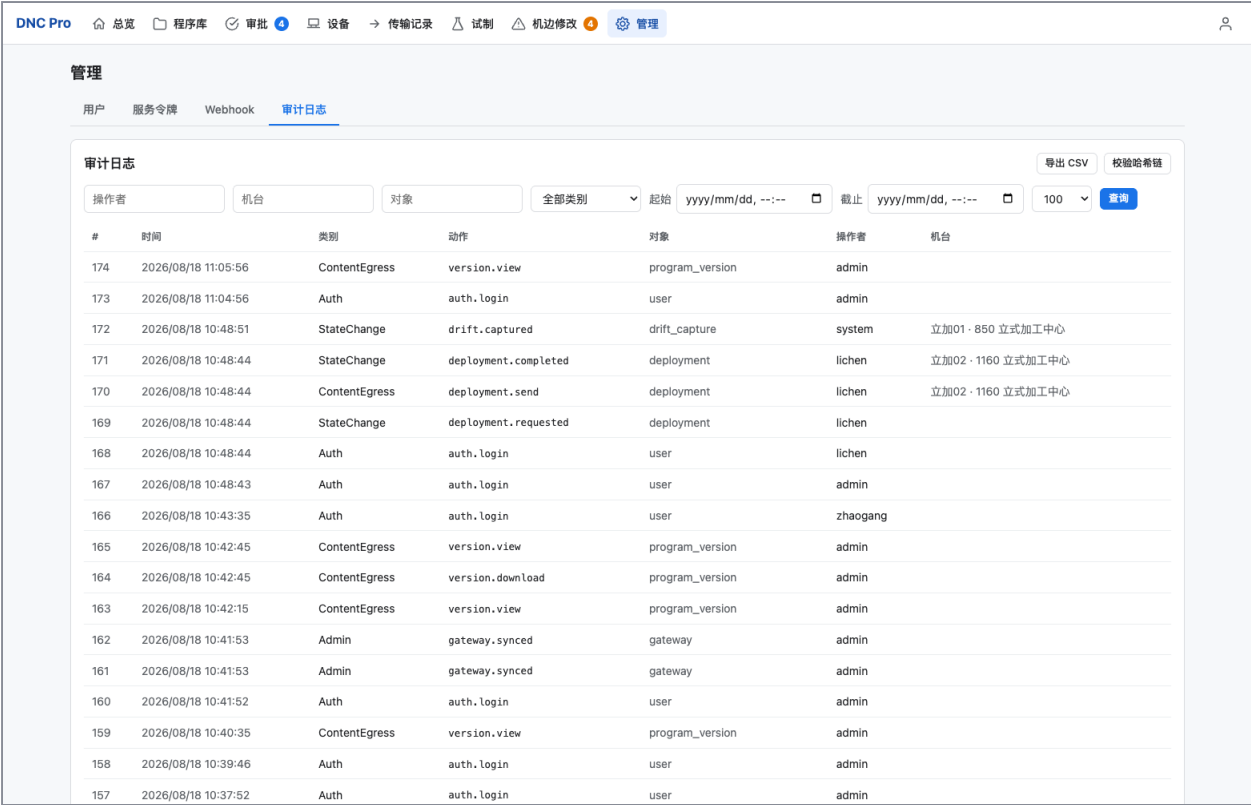


图 5-27 审计日志页面

审计日志为只增不改的哈希链，每条记录包含前一条记录的哈希值。任何一条记录被篡改或删除，其后的整条链均无法通过校验。

记录类别按表 5-29 的规定。

表 5-29 审计记录类别

类别	典型事件
StateChange（状态变更）	version.created、version.released、deployment.requested、deployment.completed、deployment.failed、drift.captured、drift.rejected
ContentEgress（内容外流）	version.view、deployment.send

类别	典型事件
Admin / Auth（管理与认证）	service_token.created、webhook.created、gateway.synced、auth.login

每条记录包含序号、时间、操作者（人员或令牌）、代理操作人、客户端 IP、对象类型与 ID、变更前后的 JSON、涉及的机台与网关。

5.9.5.1 查询与导出

操作步骤：

- a) 在页面顶部按操作者、机台、对象、类别、时间段设定筛选条件；
- b) 核对筛选结果；
- c) 单击「导出 CSV」下载当前筛选结果，用于向质量部门或客户提交。

5.9.5.2 哈希链校验

操作步骤：单击「校验哈希链」，系统自创世记录起重算整条链。

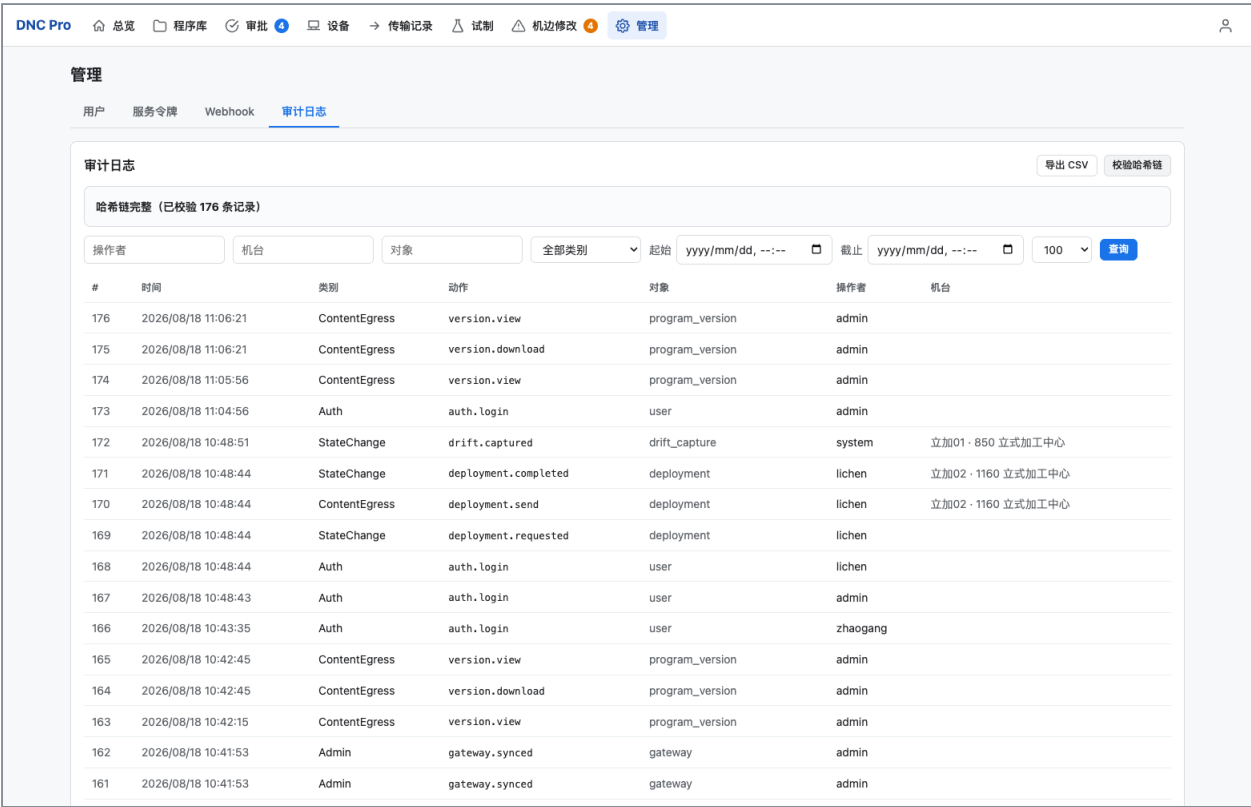


图 5-28 哈希链校验结果

校验通过时显示「哈希链完整（已校验 N 条记录）」；链不完整时给出第一条断裂记录的序号。

说明

留存日志与证明日志未被篡改是两个不同的能力。应对客户审核或体系认证时，哈希链校验结果是后者的直接证据。

5.9.6 权限要求

表 5-30 系统管理相关权限

操作	所需权限	具备该权限的角色
用户与授权管理、令牌管理、Webhook 管理	admin	管理员
查阅与导出审计日志、校验哈希链	admin	管理员

6 参考资料

本章为查证性内容，规定角色权限、机床系统差异、REST API 接口、日常核查要求与术语定义。 各节内容按表 6-1 索引。

表 6-1 参考资料索引

条款	内容
6.1 角色与权限	五个角色与十三项权限的完整矩阵，以及授权范围的判定规则
6.2 机床系统差异	FANUC、西门子、三菱、兄弟的文件系统语义差异及其处理方式
6.3 REST API	认证方式、错误约定、端点总览与集成示例
6.4 日常核查	日常状态查看、备份确认、机床恢复、账号凭据与月度核查
6.5 术语表	本说明书使用的术语、英文对照与规范用词

6.1 角色与权限

6.1.1 适用范围

本节规定本系统的访问控制模型。适用于管理员配置授权，亦作为其他各节权限要求的判定依据。

6.1.2 设计原则

- a) **角色固定，不可自定义。** 五个角色对应车间中实际存在的五类职责。可自定义角色的系统在实践中会退化为每人一个角色，失去审计意义；
- b) **范围可变。** 同一角色可仅作用于某个机组或某个程序库；
- c) **人员与令牌适用同一套规则。** 不存在越权令牌。

6.1.3 权限矩阵

角色与权限的对应关系按表 6-2 的规定。

表 6-2 角色与权限矩阵

权限	只读	操作工	编程员	审批员	管理员
programs.read 查阅程序与元数据	✓	✗	✓	✓	✓
programs.read.released 仅查阅已发布版本	✓ ^a	✓	✓ ^a	✓ ^a	✓
programs.content.view 查阅、下载正文	✗	✗	✓	✓	✓
programs.write 建程序、传版本、建分配	✗	✗	✓	✗	✓
versions.submit 提交审批	✗	✗	✓	✗	✓
approvals.decide 批准、驳回	✗	✗	✗	✓	✓
deployments.send.released 下发已发布版本	✗	✓	✓	✗	✓
deployments.send.proveout 下发试制版本	✗	✗	✓	✗	✓
drift.disposition 处置机边修改	✗	✗	✓	✗	✓

权限	只读	操作工	程序员	审批员	管理员
<code>machines.read</code> 查阅机台与文件状态	✓	✓	✓	✓	✓
<code>machines.files.restore</code> 还原快照	✗	✗	✓	✗	✓
<code>machines.files.adopt</code> 采纳未受管文件	✗	✗	✓	✗	✓
<code>admin</code> 用户、令牌、Webhook、审计	✗	✗	✗	✗	✓

^a 具备完整读权限 `programs.read` 的角色隐含具备仅读已发布版本的能力。

6.1.4 角色职责

五个角色的对应岗位与职责范围按表 6-3 的规定。

表 6-3 角色职责

角色	对应岗位	职责范围
只读	生产计划、班组长	查阅程序与机台，不可查阅正文，不可执行任何变更
操作工	车间工位	查阅已发布版本，向本机组机床下发正式版本，不可查阅正文
程序员	工艺工程师	编写程序、提交审批、下发（含试制）、处置机边修改、还原快照与采纳文件
审批员	工艺主管、质量工程师	查阅正文、批准或驳回。不可编写，不可下发
管理员	系统管理员	上述全部，另含用户、令牌、Webhook 与审计管理

注意

程序员不具备批准权限，审批员不具备下发权限，二者构成职责分离的基本结构。管理员同时具备两类权限，因此生产环境中的管理员账号数量应尽量少，且不应用于日常操作。

6.1.5 授权范围

每条授权由「角色 × 范围」构成，范围类型按表 6-4 的规定。

表 6-4 授权范围类型

范围	作用对象
全局	全部对象
机组	该机组内的机台，及与之相关的下发、机边修改处置、快照操作
程序库	该程序库内的程序、版本与审批

一名用户可持有多条授权，其有效权限为各条授权的并集。

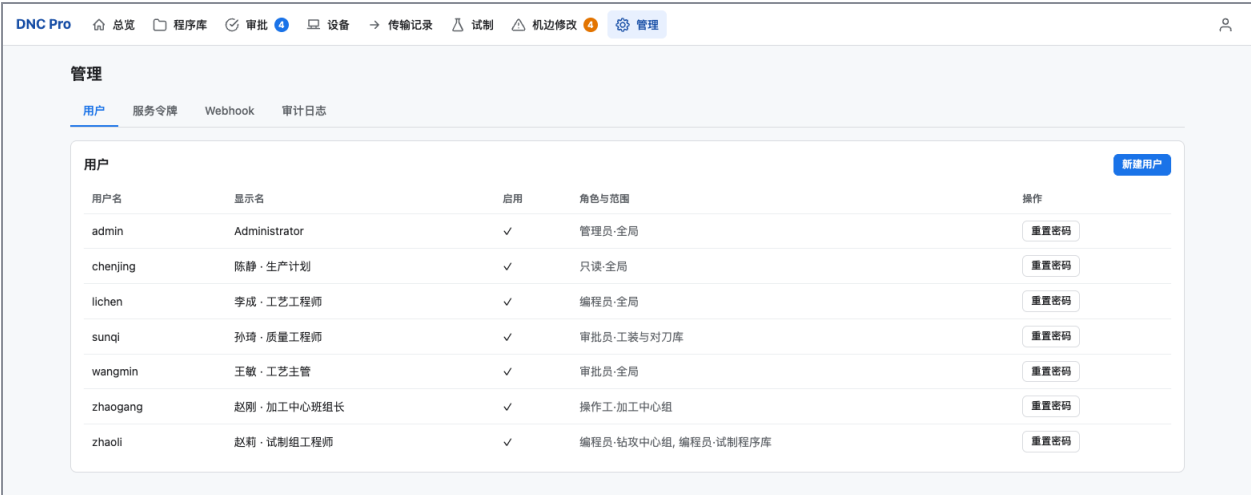


图 6-1 用户与授权页面

6.1.5.1 判定示例

以赵莉为例，其授权为「编程员·试制程序库」与「编程员·钻攻中心组」两条， 各项操作的判定结果按表 6-5 的规定。

表 6-5 授权判定示例

操作	判定结果	原因
在试制程序库上传新版本	✓	程序库范围覆盖
在量产程序库上传新版本	✗	范围不覆盖，返回 403
将试制库的程序下发至钻攻 01	✓	机组范围覆盖
将试制库的程序下发至立加 01（加工中心组）	✗	机组范围不覆盖，返回 403
处置钻攻 01 上的机边修改	✓	机组范围覆盖
批准本人创建的版本	✗	不具备 approvals.decide

6.1.6 与审批策略的关系

访问控制决定操作是否被允许，程序库审批策略决定放行所需的人数。两者相互独立：

- a) 具备 `approvals.decide` 但程序库要求 2 人审批时，单次批准仅计一票；
- b) 程序库启用「禁止自审自批」时，即使具备权限，作者本人的批准也不计入。

审批策略的配置见 5.2。

6.1.7 服务令牌

服务令牌适用与人员账号完全相同的角色与范围模型。令牌特有的两项属性（可代理身份、高危需操作人）见 5.9。

6.1.8 权限相关错误码

表 6-6 权限相关错误码

状态码	含义	排查方向
403	当前角色或范围不覆盖该目标对象	检查用户的授权范围
409	权限满足，但对对象当前的生命周期状态不允许该操作，例如下发草稿版本	检查对象状态

6.2 机床系统差异

6.2.1 适用范围

本节规定各厂商控制系统在文件命名、目录与程序号方面的语义差异，以及本系统的处理方式。适用于配置机台分配与排查下发异常。

本系统内置厂商画像表，按机台的控制系统与型号自动选用。日常使用中无需人工干预， 本节内容用于异常排查。

6.2.2 画像对照表

各控制系统的能力差异按表 6-7 的规定。

表 6-7 控制系统能力对照

能力	FANUC 现代 (0i-D/0i-F/30i/31i/32i/35i)	FANUC 传统	西门子	三菱	兄弟 S 系	兄弟 TC 系
支持子目录列表	√	×	√	×	√	√
支持指定目录	√	×	√	√	√	×
程序名取自内容	√	√	×	×	×	×
列表去除 O 号前导零	√	×	×	×	×	×
必须带扩展名	×	×	√	×	×	×
支持程序号锁定区间	√	√	×	√	×	×
默认根目录	//CNC_MEM/	机床当前前台目录	/nckfs	PRG\USER\	/	/

6.2.3 FANUC 程序名规则

FANUC 控制器在接收文件时忽略传入的文件名参数，程序名取自内容，即第一个换行符与第二个换行符之间的一行，见图 6-2。

%	← 第 1 行
01001(PUMP BODY ROUGH)	← 名称行：01001

G17 G21 G40 G49 G80 G90

图 6-2 FANUC 程序名的 O 号形式

尖括号形式同样有效，见图 6-3。

```
%
<PUMPROUGH>
G17 G21 ...
```

图 6-3 FANUC 程序名的尖括号形式

警告

若内容中的程序名为 05，而机台文件名配置为 01001 且未设置名称改写，该程序将在机床上落地为 05。向 FANUC 机床建立分配时，应将「程序名改写」设为与机台文件名一致的 O 号。本系统在发送前改写名称行，同时保留原有的括号注释。分配配置方法见 5.3。

6.2.3.1 O 号前导零

标准 O 号在不同接口下的写法不一致：

- a) 现代 FANUC 在列目录时去除前导零，00010 显示为 010；
- b) 传统 FANUC 在列目录时按存储时的写法显示，但 readProgramInfo 接口仍去除前导零。

本系统在匹配与比对时将 00010、0010、o10 统一归一为 010，因此配置值为 01 而机床显示为 00001 不会导致失配。

非 O 号形式的名称（如 SAMPLE、<NAME>）按原样处理，区分大小写。

6.2.4 西门子

注意

西门子的 NC 文件必须带扩展名（.MPF 为主程序，.SPF 为子程序）。机台文件名未填写扩展名时，落地将失败。

默认根目录为 /nckfs，支持子目录。

6.2.5 三菱

默认根目录为 PRG\USER\（使用反斜杠）。支持指定目录，但不支持列出子目录，本系统仅列出根目录下的文件。

6.2.6 兄弟

兄弟系统按型号区分：S 系列（如 S700X1）支持指定目录；TC 系列（如 TC-S2D）不支持，填写的目录不生效，文件落至根目录。本系统按型号自动选用对应画像。

6.2.7 程序号锁定区间

FANUC 与三菱支持将某一 O 号区间设为受保护区间（例如 O8000~O8999 存放厂商宏）。向锁定区间内写入将失败。

本系统在下发的预检阶段检查该项，在机床被改动之前终止事务，此时传输记录中「失败阶段 = 预检」、「回滚 = 无需回滚」，见 5.4。

6.2.8 归一化比对

下发第 ⑥ 阶段的校验按上述画像执行归一化，吸收下列无害差异：

- a) 行结束符差异；
- b) FANUC 的 O 号前导零；
- c) 末尾空行的增删。

归一化仅吸收控制器已知的无害变换，真实的内容差异必定被检出。

6.2.9 未列出的控制系统

彼络物联网支持的机床系统不限于本节所列。未匹配到具体画像的系统采用保守的通用画像：不假定支持子目录、不假定支持指定目录、不执行名称改写。此类机床通常可正常工作，但无法使用上述针对性处理。

说明

机床的实际行为与画像不符时，可将传输记录中的失败阶段与失败详情（见 5.4）反馈给供应方。画像表可以扩充。

6.3 REST API

6.3.1 适用范围

本节规定本系统对外提供的 REST 接口。适用于与 MES、CAM、看板等上层系统的集成开发。

管理控制台与机边操作台均为本套接口的客户端，不存在未公开接口。界面上可执行的操作，接口均可执行。

接口文档入口：

a) 交互式参考：<http://<主机>:8030/api/docs>；

b) OpenAPI 3.1 文档：<http://<主机>:8030/openapi/v1.json>。

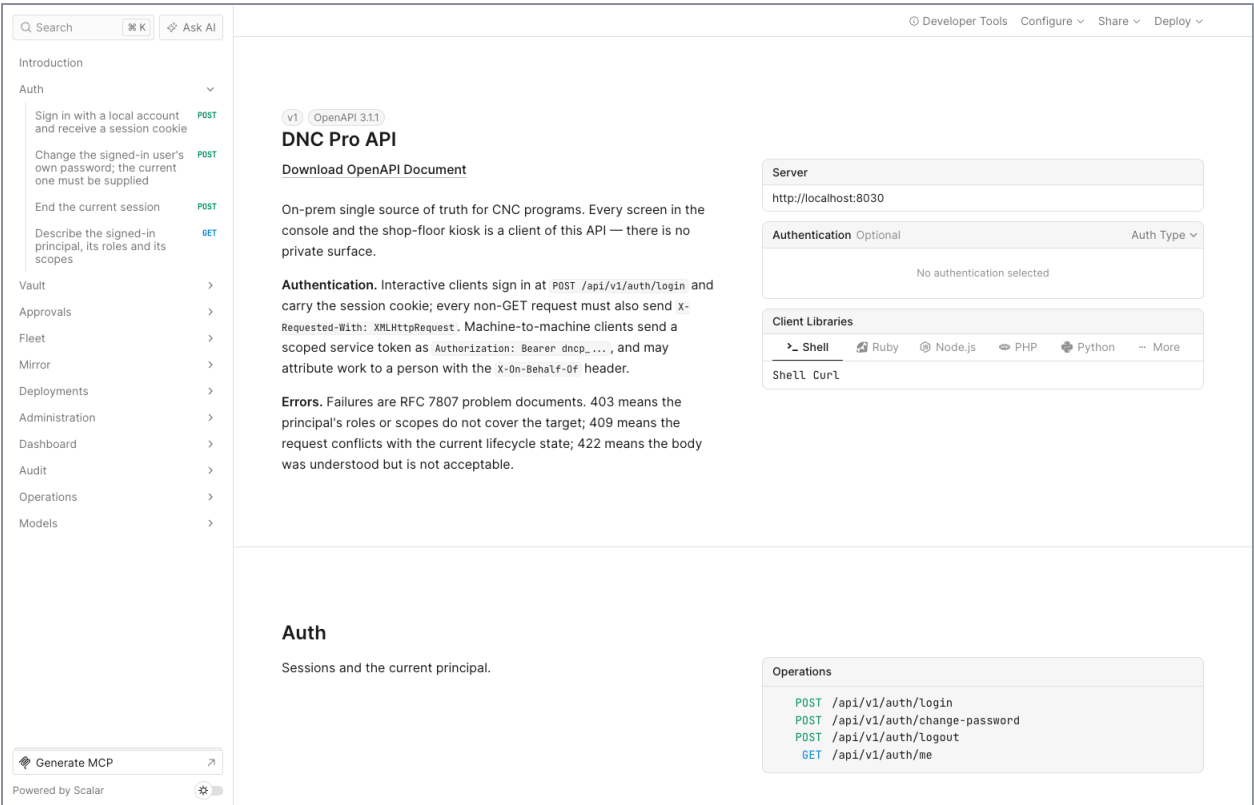


图 6-4 REST API 交互式参考页面

说明

每个接口均附摘要、分组标签与错误响应说明。该约束由构建时的测试强制执行，接口缺少文档时构建失败。

6.3.2 认证

6.3.2.1 浏览器客户端

登录请求：

```
POST /api/v1/auth/login
Content-Type: application/json

{ "username": "lichen", "password": "..."}

```

登录成功后种下会话 Cookie。

注意

所有非 GET 请求必须携带 X-Requested-With: XMLHttpRequest 请求头，否则被拒绝。该头用于 CSRF 防护：XHR 请求可携带该头，跨站表单提交不能。

6.3.2.2 机器对机器

使用服务令牌（见 5.9）：

```
Authorization: Bearer dncp_<id>_<secret>

```

可另行声明实际操作人，使审计记录可追溯到具体人员：

```
X-On-Behalf-Of: lichen

```

令牌启用「高危需操作人」时，下发、删除等操作必须携带该请求头，否则拒绝执行。

6.3.3 错误约定

失败响应统一返回 RFC 7807 problem document，状态码按表 6-8 的规定。

表 6-8 错误状态码

状态码	含义	排查方向
400	请求本身不合法	检查请求体与参数格式

状态码	含义	排查方向
401	未认证、会话过期或令牌无效	检查凭据与有效期
403	角色或授权范围不覆盖目标对象	检查授权配置（见 6.1）
404	对象不存在，或在当前范围内不可见	检查对象 ID 与授权范围
409	与对象当前的生命周期状态冲突，例如下发草稿版本	检查对象状态
422	请求可被理解，但内容不可接受	检查业务约束
503	服务暂不可用	稍后重试，持续出现时报请系统维护人员处理

403 与 409 为集成过程中最常见的两类错误：403 应检查授权，409 应检查对象状态。

6.3.4 端点总览

表 6-9 端点总览

分组	主要端点
Auth	POST /api/v1/auth/login、POST /auth/logout、POST /auth/change-password、GET /auth/me
Vault	POST/GET /libraries、POST/GET /programs、POST/GET /programs/{id}/versions、POST /versions/{id}/submit、GET /programs/{id}/diff、GET /versions/{id}/content、POST /versions/{id}/obsolete
Approvals	GET /approvals、POST /approvals/{id}/decide
Fleet	POST/GET /gateways、POST /gateways/{id}/sync、GET/PATCH /machines/{id}、POST/GET/PATCH /machine-groups、GET /machines/{id}/files、POST /machines/{id}/request-checkin
Assignments	POST/GET /machine-assignments、POST /machine-assignments/{id}/preview-transform

分组	主要端点
Deployments	POST/GET /deployments、GET /deployments/{id}
Trials	GET /trials、POST /trials/{id}/promote、POST /trials/{id}/pull-back
Mirror / Drift	GET /drift、POST /drift/{id}/accept、POST /drift/{id}/reject、POST /machine-files/{id}/adopt、POST /machines/{id}/adopt-all、GET /machine-files/{id}/snapshots、POST /machine-files/{id}/restore
Admin	POST/GET /admin/users、POST/GET /admin/service-tokens、POST/GET /admin/webhooks、GET /admin/webhooks/deliveries
Audit	GET /audit、GET /audit/export、GET /audit/verify
Dashboard	GET /dashboard/summary、GET /dashboard/recent-deployments

6.3.5 集成示例

6.3.5.1 CAM 后处理自动上传版本

```

TOKEN="dncp_...."
BASE="http://dncpro.shop.local:8030"

# 1. 上传新版本（内容以 base64 传入）
VERSION=$(curl -fsS -X POST
"$BASE/api/v1/programs/$PROGRAM_ID/versions" \
-H "Authorization: Bearer $TOKEN" \
-H "X-On-Behalf-Of: lichen" \
-H "Content-Type: application/json" \

```

```
-d "{\"contentBase64\":\"\\\"$(base64 -w0 01001.nc)\\\"\", \"notes\":\"CAM 自动出图 · 工单 W0-88213\\\"}\"")
```

```
VERSION_ID=$(echo "$VERSION" | jq -r .id)
```

2. 提交审批（自动放行的程序库将直接转为已发布）

```
curl -fsS -X POST "$BASE/api/v1/versions/$VERSION_ID/submit" \
  -H "Authorization: Bearer $TOKEN" -H "X-On-Behalf-Of: lichen"
```

6.3.5.2 MES 按工单批量下发

```
curl -fsS -X POST "$BASE/api/v1/deployments" \
  -H "Authorization: Bearer $TOKEN" \
  -H "X-On-Behalf-Of: zhaogang" \
  -H "Content-Type: application/json" \
  -d '{
    "versionId": "01a012b7-....",
    "assignmentIds": ["01a012b8-....", "01a012b8-...."],
    "isTrial": false,
    "trialHours": null
  }'
```

响应返回批次 ID 与每台机台的下发 ID。可逐个轮询 GET /deployments/{id} 直至 status 变为 Succeeded 或 Failed，亦可订阅 deployment.completed 与 deployment.failed Webhook 以免除轮询，见 5.9。

6.3.5.3 看板读取总览数据

```
curl -fsS "$BASE/api/v1/dashboard/summary" -H "Authorization:
Bearer $TOKEN"
```

```
{
  "gatewaysTotal": 2,
```

```
"gatewaysUnreachable": 0,  
"machinesWithMirrorError": 1,  
"pendingApprovals": 4,  
"openDrift": 4,  
"activeTrials": 2,  
"failedDeployments24h": 1  
}
```

6.3.5.4 质量追溯：导出指定机台的审计记录

```
# 查询与导出的筛选参数: principalName、machine、entityType、entityId、  
category、from、to  
curl -fsSG "$BASE/api/v1/audit/export" \  
  --data-urlencode "machine=立加01 . 850 立式加工中心" \  
  --data-urlencode "from=2026-08-01" \  
  --data-urlencode "format=csv" \  
  -H "Authorization: Bearer $TOKEN" -o audit.csv  
  
curl -fsS "$BASE/api/v1/audit/verify" -H "Authorization: Bearer  
$TOKEN"  
# {"intact":true,"checked":165,"firstBrokenSeq":null}
```

6.3.6 版本策略

路径中的 v1 为契约版本。向后兼容的新增（新增字段、新增端点）在 v1 内进行；破坏性变更启用 v2，并在过渡期内与 v1 同时提供。

6.4 日常核查

6.4.1 适用范围

本节规定使用单位在日常使用中应执行的核查与维护工作。全部工作经管理控制台完成，适用于系统管理员。

6.4.2 日常状态查看

每个工作日应查看一次总览页。各项指标的含义与处理措施按表 6-10 的规定。

表 6-10 总览页关注项

关注项	含义	处理措施
不可达网关	该网关当前无法访问，其下全部机台既不能下发也不能备份	检查网关供电与网络，见 7.2.1
镜像异常机台	该机台最近一轮备份失败	按行内显示的原因处理，见 7.2.2
24 小时内失败的下发	存在下发未成功的机台	查看传输记录判定机床上的实际内容，见 7.3.1
待审批版本、待处置机边修改	存在等待人工处置的事项	转交相应责任人处置

警告

不可达网关与镜像异常应在当班内处理。该状态持续期间，相关机床既无新的备份，也不再进行机边修改检查，控制器数据丢失时将无近期快照可供还原。

6.4.3 备份

本系统的备份分为两层，分工按下列规定：

- a) 机床侧内容由滚动镜像持续备份，形成历史快照，使用单位无需另行操作，见 5.6；
- b) 本系统自身的数据（程序库、版本内容、审批与审计记录）按交付时约定的策略定期备份。

警告

备份默认存放于本系统所在的服务器上。服务器整机故障时该备份同时失效。使用单位应确认备份已同步至本系统主机之外的存储，并定期确认该同步仍在执行。

系统自身数据恢复完成后，应逐台核对机台的「最近校验」是否重新开始更新。

6.4.3.1 恢复被清空的机床

机床控制器数据被清空且本系统数据完好时，操作步骤：

- a) 进入「设备 → 机台 → 文件」，逐个文件执行「快照 → 还原」；
- b) 受管文件亦可直接重新下发最新的已发布版本。

注意

还原经由与下发相同的事务式管线执行，执行前应确认机床未处于加工状态。

还原规则见 5.6。

6.4.4 账号与凭据

- a) 首次登录后应立即修改交付时提供的管理员初始密码；
- b) 管理员账号数量应尽量少，且不应用于日常操作。日常操作应使用程序员或审批员账号；
- c) 集成应一律使用服务令牌，按最小范围授权并设定有效期，见 5.9；
- d) 网关侧应为本系统建立专用账号与密钥，不应复用网关管理员账号，见 4.1.2；
- e) 人员离职或转岗时应及时停用其账号，并吊销其名下的服务令牌。

6.4.5 定期核查

每月执行一次，按表 6-11 逐项核查。

表 6-11 月度核查项

核查项	核查方法	合格判据
网关状态	总览页	不可达网关数为 0
机台备份状态	设备页	镜像异常机台数为 0，全部机台的「最近校验」处于近期
审计链完整性	管理 → 审计 → 校验哈希链	结果为完整
Webhook 投递	管理 → Webhook → 投递记录	无长期积压的失败投递

核查项	核查方法	合格判据
账号与令牌	管理 → 用户	离职人员账号已停用，无过期未清理的服务令牌
系统数据备份	按交付时约定的方式确认	近 30 天备份存在，且已同步至异地

核查中发现的异常应按第 7 章的相应条款处置。

6.5 术语表

6.5.1 适用范围

本节规定本说明书使用的术语及其定义。正文各章的用词以本节为准； 本节与其他各节表述不一致时，以本节为准。

6.5.2 程序相关术语

表 6-12 程序相关术语

术语	英文	定义
程序库	Library	审批策略的施加单位，规定其下程序所需的审批人数、能否自审自批、是否自动放行
程序	Program	一个零件一道工序的加工程序。由名称、零件号、工序、适用机型构成其身份
版本	Version	程序的一次具体内容。内容在上传后不可变更，仅状态可变
变体分组	Variant Group	零件号与工序相同的多个程序（如 FANUC 版与西门子版）在界面上的归组显示。变体之间不合并
来源	Origin	版本的产生方式，取值为上传、机边捕获、采纳
内容哈希	Content Hash	版本内容的 SHA-256 值。内容相同的版本仅存储一份，该值为内容一致性的判定依据

6.5.3 设备相关术语

表 6-13 设备相关术语

术语	英文	定义
网关	Gateway	彼络物联网关。本系统经由网关与机床通信，不直接连接机床

术语	英文	定义
机台	Machine	一台数控机床在本系统中的记录。台账由网关同步产生
机组	Machine Group	授权与策略的施加单位，规定可操作该组机台的人员范围及是否允许试制。机组不表示物理位置
孤立机台	Orphaned	曾经同步过、但已不存在于网关配置中的机台。保留历史记录，不再对其执行任何操作
严格模式	Strict Mode	机台级开关。启用后在文件列表中高亮标记未受管文件，仅作参考，不阻断任何操作
最近校验	Last Verified	该机台最近一次被滚动镜像完整扫描完成的时刻。未完成的轮次不更新该值

6.5.4 下发相关术语

表 6-14 下发相关术语

术语	英文	定义
机台分配	Assignment	程序与机台的绑定关系，规定落地文件名、目录与落地转换规则
落地转换	Transform	发送前对版本内容执行的处理，包括程序名改写、%包裹、行结束符转换与目标编码转换
事务式下发	Transactional Transfer	由预检、快照、删除、发送、回读、校验六个阶段构成的下发管线，任一阶段失败自动回滚快照
回读	Readback	将刚写入机床的内容读回。回读内容与发送内容比对一致是判定下发成功的必要条件
归一化比对	Normalized Comparison	按厂商画像吸收无害差异（行结束符、O 号前导零、末尾空行）后进行的内容比对
回滚	Restore	下发失败时以快照恢复机床原有内容。结果取值为无需回滚、已回滚、回滚失败

术语	英文	定义
批次	Batch	一次操作产生的一组下发任务（同一版本发往多台机台）。各机台的成败相互独立
试制	Trial / Prove-out	限时的验证性下发。全程带试制徽标，到期后仍需人工转正或撤回

6.5.5 镜像与机边修改相关术语

表 6-15 镜像与机边修改相关术语

术语	英文	定义
滚动镜像	Rolling Mirror	轮转扫描全部机台、备份每台机床上每个文件的后台循环。执行时向真实下发任务让路
快照	Snapshot	某个机床文件在某一时刻的内容副本。按产生方式分为下发前快照、回读快照、镜像快照
受管文件	Managed	有机台分配指向的机床文件
未受管文件	Unmanaged	无机台分配指向的机床文件。同样被备份和保护，但不被检查或纠正
采纳（未受管文件）	Adopt	将机床上的未受管文件收入程序库，以其当前内容作为 v1
机边修改	Drift	受管文件在机床侧被改动的情形。本系统自动将其捕获为待处置的草稿版本
处置	Disposition	对机边修改作出的决定，取值为采纳（进入发布流程，机台内容不变）或拒绝（可选推回受控版本）
推回	Push Back	拒绝机边修改时，将已发布版本重新下发到机床的操作。该操作需显式勾选

6.5.6 权限与审计相关术语

表 6-16 权限与审计相关术语

术语	英文	定义
角色	Role	固定的五种身份：只读、操作工、编程员、审批员、管理员
范围	Scope	授权的作用域，取值为全局、机组、程序库
职责分离	Separation of Duties	版本作者不得批准自己创建的版本。该约束默认启用
服务令牌	Service Token	机器对机器集成使用的凭据，格式为 <code>dncp_<id>_<secret></code> ，适用与人员账号相同的权限规则
代理身份	On-Behalf-Of	令牌声明本次操作的实际发起人，使审计记录可追溯到具体人员
内容外流	Content Egress	程序正文的任何一次查看或下载。单独记入审计
哈希链	Hash Chain	每条审计记录包含前一条记录哈希的链式结构。任何篡改都将导致其后的链校验失败

6.5.7 规范用词

同一概念在本说明书中只使用一种称谓。表 6-17 规定规范用词及其不再使用的同义表述。

表 6-17 规范用词与不推荐用词

规范用词	不推荐用词	说明
机台	机床（指系统记录时）	「机台」指本系统中的设备记录；「机床」仅指车间中的物理设备
下发	传输、推送、拷贝	「下发」为业务动作的统称
发送	—	仅指下发事务的第 ④ 阶段，不作为下发的同义词使用
传输记录	下发记录、传输日志	界面名称，指控制台中的传输记录页面
机边修改	漂移、drift	统一使用「机边修改」
试制	试切、prove-out	统一使用「试制」；涉及车间口语场合可在首次出现时附注「(试切)」

规范用词	不推荐用词	说明
滚动镜像	备份轮询、镜像任务	指后台备份机制本身
快照	备份副本	指某一时刻的内容副本
已发布	正式版、放行版	版本状态名称
机组	机台分组、班组	授权与策略单位

7 常见问题与故障处置

7.0 适用范围

本章按功能分类给出常见故障现象、可能原因与处理措施，以及使用中的常见问题说明。本章为处置性内容，各项措施的完整规则见其引用的条款。

7.1 访问与登录

7.1.1 打不开管理控制台

处理措施。按下列顺序逐项排查：

- a) 核对地址是否与实施人员提供的一致，包括端口号，见 4.0.2；
- b) 确认本机与本系统处于同一局域网内，办公网与车间网分隔时应使用车间网络；
- c) 换用其他计算机或触摸屏访问，判断是本机问题还是系统问题；
- d) 全部终端均无法访问时，应报请系统维护人员处理。

7.1.2 管理员密码丢失

处理措施。

- a) 存在其他可用的管理员账号时，由该账号在「管理 → 用户」中重置密码，见 5.9；
- b) 全部管理员账号均无法登录时，应报请系统维护人员处理，不应通过其他途径自行绕过登录。

注意

管理员账号不应仅设置一个。应至少保留两个管理员账号，避免单一账号失效导致无法管理系统。

7.1.3 页面可打开，但程序上传总是失败

原因。程序内容的存储不可写。

处理措施。该故障在使用侧无法自行排除，应报请系统维护人员处理。

警告

程序内容存储不可写时，界面显示完全正常，但每一次上传与每一次镜像捕获都会静默失败。故障期间不得以界面显示为准判断程序已保存，恢复后应重新上传并确认版本存在。

7.2 网关与机台

7.2.1 注册网关后同步不到机台

处理措施。按下列顺序逐项排查：

- a) 确认本系统与该网关之间网络可达。排查时应以本系统所在的网络位置为准，操作人员个人电脑能打开网关页面并不说明本系统也能连通；
- b) 确认网关地址填写为 `http://<IP>`，网关 HTTP 服务监听 80 端口，地址不应带路径；
- c) 确认认证方式与密钥匹配。网关侧启用安全控制时必须填写密钥；
- d) 确认网关侧的对应用户仍存在，且密钥未被重新生成。

网关注册方法见 4.1.3。

7.2.2 机台的「最近校验」持续不更新

原因与处理措施。行内显示的失败信息与对应原因按表 7-1 的规定。

表 7-1 镜像失败信息与原因

行内显示	可能原因	处理措施
Machine offline.	机床关机、网线松脱、网关侧该机台被停用	检查机床电源与网络，检查网关侧机台状态
No permission.	网关侧密钥失效或权限不足	按 4.1.2 重新生成密钥
持续显示「从未校验」	机台刚同步进入，尚未完成首轮扫描	等待数十秒至数分钟，时长取决于机队规模

说明

「最近校验」仅在完整扫完一台机床后更新。该时刻不更新表示确实未完成备份，不表示部分文件备份成功，见 5.6。

7.2.3 机床改名或增减后如何处理

重新执行一次「同步机台」。同步操作具备幂等性。网关配置中已不存在的机床被标记为孤立，保留历史记录但不再被操作，见 4.1.4。

7.3 程序下发

7.3.1 下发失败后机床上的实际内容

处理措施。查看传输记录中的两列，按表 7-2 判定。

表 7-2 下发失败后的机床内容判定

传输记录显示	机床上的内容	处理措施
失败阶段为「预检」或「快照」	未被改动	排查网络与机床状态后重新下发
回滚结果为「已回滚」	为原有版本	生产可继续，排除故障后重新下发
回滚结果为「回滚失败」	不确定	应到机边人工核对后方可恢复生产

警告

回滚结果为「回滚失败」的文件处于内容未知状态，应在恢复生产前由具备机床操作资质的人员到机边核对实际程序内容，见 5.4。

7.3.2 发送至 FANUC 后程序号不正确

原因。FANUC 控制器忽略传入的文件名，程序名取自内容中的名称行。

处理措施。在机台分配中将「程序名改写」设为目标 O 号，见 5.3 与 6.2。

7.3.3 发送至西门子失败

原因。西门子的 NC 文件必须带扩展名（.MPF 或 .SPF）。

处理措施。检查机台文件名是否缺少扩展名，见 6.2。

7.3.4 预检阶段即失败

原因。预检校验机床可达性、程序号未被锁定、分配有效。程序号被锁定在 FANUC 与三菱上较常见，厂商宏通常占用 O8000~O8999 等受保护区间。

处理措施。 更换目标程序号，见 6.2。

7.3.5 下发缓慢或排队时间过长

原因与处理措施。

- a) 同一台机台同一时刻仅执行一个传输任务，批量下发至同一机台时串行执行，属正常行为；
- b) 滚动镜像不会拖慢下发，它在每次网关调用前向传输让路，见 5.4；
- c) 整体缓慢时，检查网关侧负载。网关同时承担数据采集任务且负载偏高时，可适当增大滚动镜像的节流间隔。

7.4 版本与审批

7.4.1 下发按钮不可用

原因。 仅「已发布」版本可执行下发。

处理措施。 按版本当前状态处理：

- a) 草稿：执行提交审批；
- b) 待审批：由审批人批准，票数不足时界面显示已获得的批准次数；
- c) 废弃：不可下发。

版本状态规则见 5.1。

7.4.2 具备审批权限但无法批准本人创建的版本

原因。 该程序库启用了「禁止自审自批」，该项默认启用，属职责分离约束。

处理措施。 由他人审批；仅配备一名工程师的单位可停用该项，或将该程序库设为自动放行，见 5.2。

7.4.3 机边捕获的版本为何是草稿

捕获的版本已被安全保存，但尚不具备任何效力。在机边修改页面执行采纳后，该版本才进入正常的审批发布流程，见 5.7。

7.5 机边修改

7.5.1 系统是否会还原机床上的改动

不会。系统仅执行捕获、记录与排队，等待人工处置。即使工程师选择「拒绝修改」，将已发布版本推回机床仍需单独勾选，见 5.7。

7.5.2 未受管文件被修改后没有记录

原因。 未受管文件被备份但不被检查，系统对其不存在「应当是什么」的基准。

处理措施。 需要对某个文件执行检查时，将其采纳进程序库，见 5.6。

7.5.3 试制期间调整参数是否产生大量记录

不会。进行中的试制（含已过期未处置的试制）抑制该文件的机边修改捕获，改动仍被完整备份，见 5.5。

7.5.4 同一文件被多次修改

后续改动更新同一条机边修改记录，不产生多条记录，见 5.7。

7.6 权限

7.6.1 用户看不到部分机台或程序

原因。 授权范围（机组或程序库）限制了可见性。

处理措施。 在「管理 → 用户」中检查该用户的授权配置，见 6.1。

7.6.2 403 与 409 的区别

a) 403：当前角色或范围不覆盖目标对象，应检查授权；

b) 409：权限满足，但对象当前状态不允许该操作（例如下发草稿版本），应检查对象状态。

见 6.1。

7.6.3 操作工能否查看程序内容

不能。操作工不具备 `programs.content.view` 权限，可将正确的版本下发至机床，但不能查看或下载程序正文，见 5.8。

7.7 集成

7.7.1 Webhook 持续投递失败

处理措施。 在「管理 → Webhook → 投递记录」中查看 HTTP 响应码与错误信息。常见原因包括：接收端地址无法解析、防火墙拦截、接收端返回非 2xx 响应。排除故障后执行「重新投递」，见 5.9。

7.7.2 API 调用提示 CSRF 相关错误

原因。 使用 Cookie 会话的非 GET 请求必须携带 `X-Requested-With: XMLHttpRequest` 请求头。

处理措施。 机器对机器的集成不应使用 Cookie 会话，应改用服务令牌的 `Authorization: Bearer dncp_...`，该方式不受此约束，见 6.3。

7.7.3 服务令牌丢失后能否找回

不能。令牌明文仅在创建时显示一次，系统仅存储其哈希值。应吊销原令牌并新建，见 5.9。

7.8 其他

7.8.1 能否完全断网运行

可以。使用本地账号时，整套系统运行于使用单位的局域网内，全部数据存储于使用单位自有服务器，不需要任何外网连接。OIDC 单点登录为可选项，不启用即可。

7.8.2 界面是否提供英文版

提供。管理控制台与机边操作台的右上角均可在简体中文与 English 之间切换。

7.8.3 一套系统可管理几个车间

每个车间部署一台彼络物联网关，本系统侧注册多条网关记录即可，网关注册方法见 4.1.3。

修订记录

本说明书的修订情况按表 A-1 的规定。

表 A-1 修订记录

版本	日期	修订内容	编制
v1.0.0	2026-08	首次发布	深圳市彼络科技有限公司

v1.0.0 首次发布

系统功能

首个正式版本包含下列功能：

- a) **程序库**：程序库、程序、版本三层结构，版本生命周期（草稿 → 待审批 → 已发布 → 废弃），内容哈希去重，任意两版并排比对，变体分组；
- b) **审批**：程序库级策略（审批人数、禁止自审自批、自动放行），审批队列与差异评审；
- c) **设备**：多网关注册与机台同步，机组与试制策略，严格模式；
- d) **机台分配**：程序名改写、%包裹、行结束符、目标编码四项落地转换，转换预览；
- e) **事务式下发**：预检 → 快照 → 删除 → 发送 → 回读 → 校验六阶段管线，失败自动回滚快照，归一化比对；
- f) **试制**：限时试制、全界面徽标、到期不自动处理、机组级禁止试制；
- g) **滚动镜像**：全天候备份机床上的每一个文件，向真实传输让路，跳过运行中的程序，镜像失败记录到对应机台；
- h) **机边修改**：受管文件的机床侧改动自动捕获为待处置版本，采纳或拒绝（可选推回），不自动还原；
- i) **未受管文件**：完整备份与快照还原，可采纳进程序库；
- j) **权限**：五个固定角色 × 三种授权范围，本地账号与可选 OIDC，服务令牌与代理身份；
- k) **审计**：只增不改的哈希链日志，状态变更与内容外流分类，查询、CSV 导出与链完整性校验；
- l) **集成**：五类事件的签名 Webhook 与重试机制，完整的 OpenAPI 3.1 文档与交互式参考；

- m) **两个前端**：管理控制台与机边操作台，均为同一套 REST API 的客户端，支持中英文切换；
- n) **备份与恢复**：机床文件的历史快照与逐文件还原，系统数据的定时备份与保留策略。

说明书

- a) 首次发布，覆盖安全与注意事项、概述、应用背景、系统构成、接入与初始配置、操作说明、参考资料与常见问题；
- b) 全部界面截图取自可复现的演示数据集。

© BIVROST TECHONOLOGIES Company Limited / 深圳市彼络科技有限公司 · DNC Pro 手册 v1.0.0
· 联系电话：18824672282