

FANUC 机器人

密码功能设定指导手册

修订	姓名	日期
编制	刘满龙	2022/2/12
审核	张丛庆	2022/2/25
批准		

版本	更新内容	日期	姓名
V1.0	首次发布	2022/2/25	刘满龙

目 录

1.	概述.....	3
2.	作业步骤.....	3
3.	密码日志.....	11
4.	常见报警.....	12

1. 概述

密码最多由 12 个字符、数字、以及符号组合而成，用来对作业人员进行各类操作、画面访问以及参数修改进行限制。密码功能应用操作可按照图 1.1 指导流程进行操作：

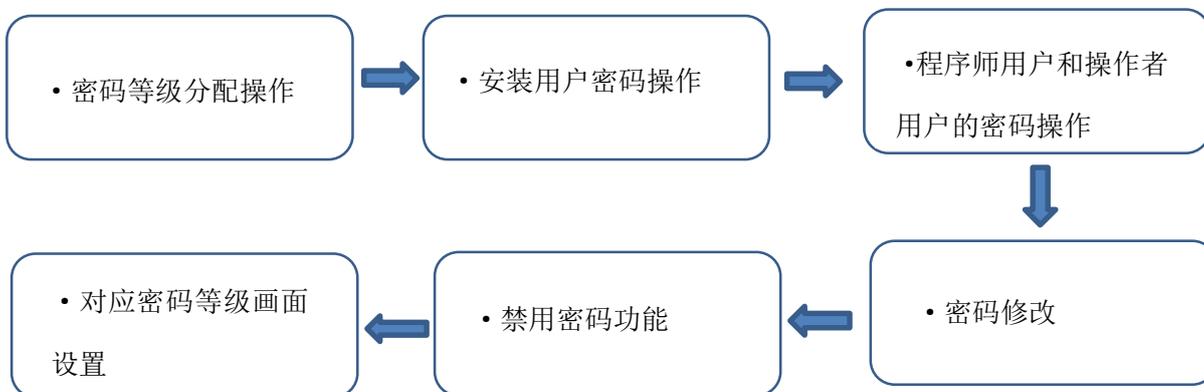


图 1.1

2. 作业步骤

2.1 密码等级的分配操作

密码有 8 种等级，每一等级允许的操作以及允许显示的画面都不同。等级 3~7 是用户定义等级，各密码等级概要如下图 2.1 所示。密码保护，只要不定义安装用户就无效。使用密码功能，首先设定安装用户，要设定安装用户，需要在分配安装用户名和密码后登入。各用户的用户名、等级以及密码，由已登入的安装用户予以分配。

等级	操作
安装	可以分配用户名、密码、以及密码等级。可以清除用户名和密码。可以设定密码日志的有效 / 无效。可以设定系统中的密码用户数。可以执行设定、程序、操作者的所有操作。 注意 安装用户只可设定 1 人。
设定者	可以执行设定系统设定中通常进行操作。
程序师	可以执行较操作者用户更加高度的操作。
操作者	可以执行基本的操作。
用户自定义	在密码设定文件中没有另行定义的情况下，可以执行基本的操作。

图 2.1

一台装置，同一时刻，最多允许登入的用户限定为一人。

标准系统中，在接通控制装置电源的时刻，或者登出后，系统返回操作者等级。

2.2 安装用户的密码操作

依次选择：菜单—6 设置—2 密码， 确认进入密码设置主页面。初始状态下，密码处于无效状态，未分配任何可用于登录的用户，如图 2.2.1 所示。



图 2.2.1

图 2.2.1 中选择登录，进入图 2.2.2 页面，提示需要首先添加安装用户才可以进行下一步操作。根据提示，输入用户名，如“FANUC1”确认后提示需要设置密码，如果是首次设置密码，旧密码无需输入，密码输入后确认，提示“密码已设置，你是否想要登录”如图 2.2.3。选择是，会登录安装用户，选择否，会处于未登录密码的状态。密码至少要三个以上字符。



图 2.2.2



图 2.2.3

上图 2.2.3 中选择“是”，出现如图 2.2.4 所示左图页面，提示当前登录的为安装用户 FANUC1，按下 F2 登录，显示右图使用者一览页面。登录时显示的@，是表示登录使用者名的标志。选择 F3 注销，手动登出当前用户，并进入图 2.2.5 所示页面，进入 Nobody 状态。



图 2.2.4

如下图 2.2.5，按下 F2 登录，进入使用者一览页面，选中需要登录的用户名，继续按下 F2 登录，提示要输入密码，图中为登录安装等级的用户。登录成功后，会处于上图 2.2.5 页面状态。



图 2.2.5

2.3 程序员用户和设定者用户的密码操作

一台装置仅可以设置一个安装用户，在设置其他等级用户时，需要首先登录安装用户。将光标移动到第二个用户名，添加设置第二个用户名，如“FANUC2”。光标移至等级栏，按下 F3 “选择”可以设置用户等级，如示教、设

置等，如图 2.3.1 所示。



图 2.3.1

如上图，如密码未设置成功，密码栏会显示“*”字符。将光标移至时间栏，输入使用者在规定时间内未进行操作时系统自动登出的超时时间，可以设置 0-10080min。设置为 0，表示不执行超时操作。系统在任何时刻，最多允许登录一位用户，如需登录其他用户，选择登录，如有其他用户已经登录，会提示是否强制注销已经登录的用户，如图 2.3.2 所示。



图 2.3.2

2.4 密码修改

需要修改密码，如图 2.4，选择 F4 密码，根据提示修改密码。密码修改无需登录安装用户等级，各等级用户均可修改当前已登录用户的密码。



图 2.4

2.5 禁用密码功能

可在已设定了密码的系统中使得密码功能无效。使得密码功能无效时，安装使用者即被清除，其他使用者不会被清除。只有安装等级使用者可以使密码功能无效，但是系统管理员换人或者忘记密码等，无法登录安装等级使用者时，可联系 FANUC 专业技术人员强制解除，在此不做介绍。



图 2.5.1

安装等级用户要使得密码功能无效，首先登录安装等级用户，在 2.5.1 左图选择 NEXT，右图按下 F3 禁用。提示是否禁用密码，选择“是”禁用后页面如图 2.5.2，密码功能即为无效。再次在图 2.5.2 右图页面登录设定安装用户后，之前设置的其他登记用户会自动出现，并不会被清除。



图 2.5.2

2.6 对应密码等级的画面限制

安装等级用户具有最高等级权限，可以进行几乎所有操作。

其他等级用户操作权限，可按如下操作进行确认：同时按住“SHIFT+DISP”按键，依次选择：8 帮助/诊断—6 Password Help，如图 2.6.1 所示。



图 2.6.1

确认进入帮助画面后，可以查看对应等级的权限。如下图 2.6.2 所示，各等级读写访问，从左按照顺序等级 7、等级 6、等级 5、等级 4、等级 3、设置等级、示教等级、生产等级分别表示是否在各画面切换菜单中允许数据输入。

其中 1：允许数据输入；0：不允许数据输入。

Top Level Menus	Sub Level Menus	Read-Write Access	Soft Part ID	Scrn ID
实用工具				
	主页	(1, 1, 1, 1, 1, 1, 1, 1)	1631	1
	声明	(1, 1, 1, 1, 1, 1, 1, 1)	153	1
	iRCalibration	(0, 0, 0, 0, 0, 0, 0, 0)	1463	1
	机器人状态	(0, 0, 0, 0, 0, 0, 0, 0)	1196	4
	程序调整	(0, 0, 0, 0, 0, 1, 0, 0)	930	1
	程序偏移	(0, 0, 0, 0, 0, 1, 0, 0)	151	1
	镜像偏移	(0, 0, 0, 0, 0, 0, 0, 0)	150	1
	工具偏移	(0, 0, 0, 0, 0, 1, 0, 0)	155	1
	坐标系偏移	(0, 0, 0, 0, 0, 1, 0, 0)	191	1

图 2.6.2

3. 密码日志

3.1 在安装用户将密码设定画面的“事件日志”条目设定为有效的情况下。

可以在密码日志中显示如下事件：

- 1) 密码事件
- 2) 编程事件
- 3) 文件操作事件等

秘密日志监视密码的登入和登出，可以确认谁登入系统，进行了什么样的修改。

只有安装用户，才可以使“事件日志”的设定有效，如图 3.1 图页面，光标移至事件日志行，按下 F4 启用，即启用密码日志事件。

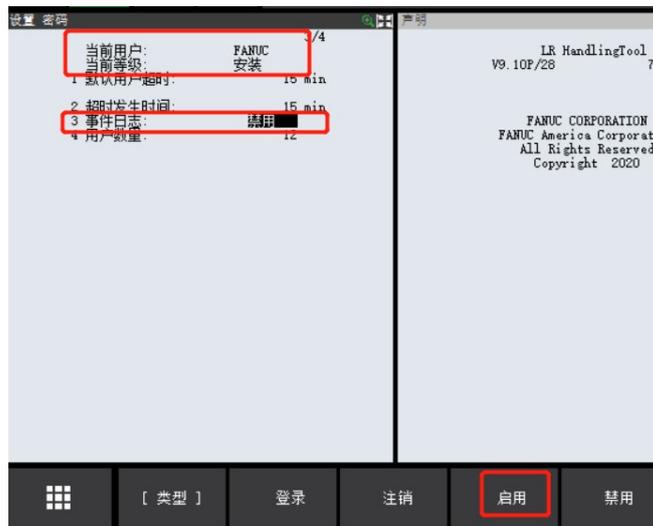


图 3.1

3.2 用户查看密码日志，需要安装、程序师、设定者的任一等级登入系统才可以查看密码日志。

依次选择：菜单—4 报警—5 密码日志，确认进入密码日志查看页面，如图 3.2 所示。

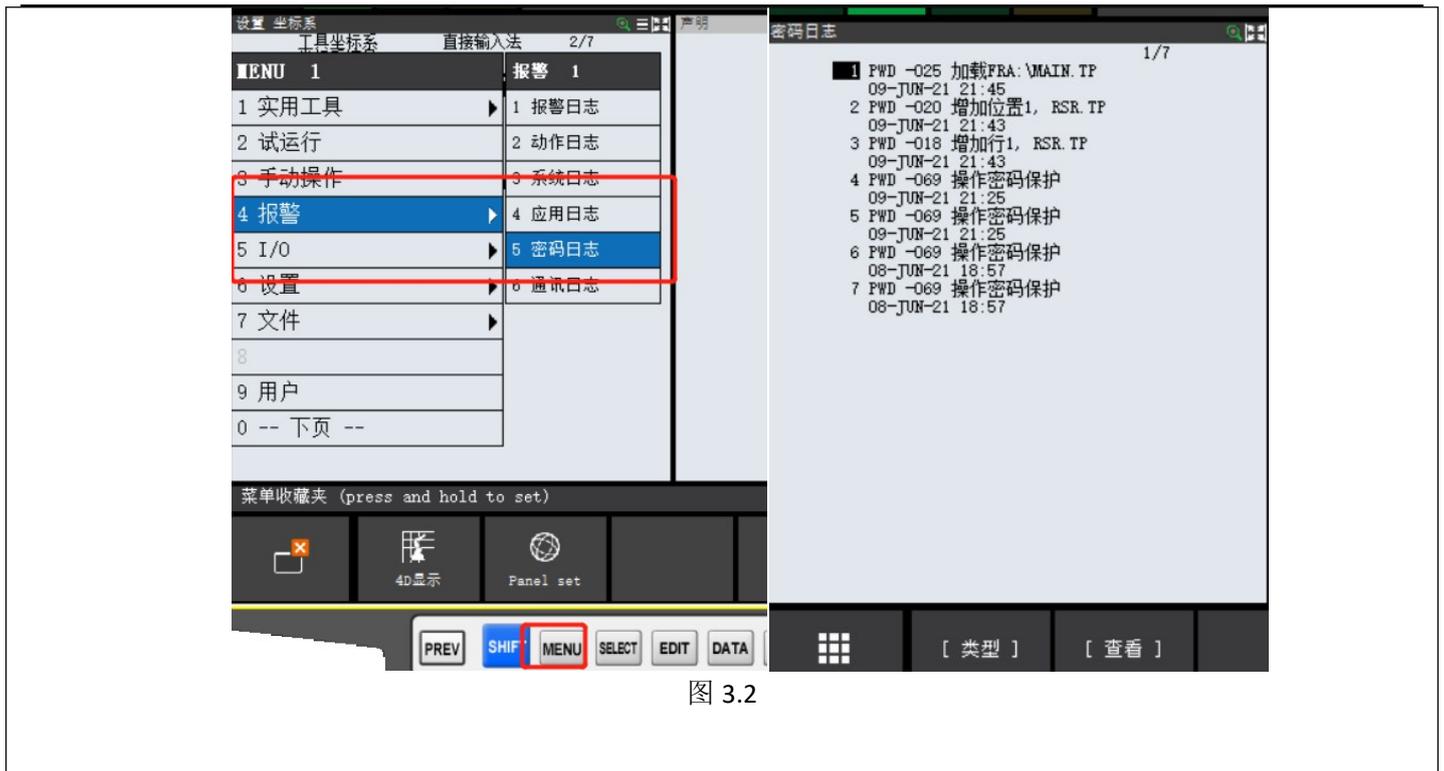


图 3.2

4. 常见报警

1) HOST-197 WARN TLNT:无效的登录 id

[原因]输入的登录 ID 无效。

[对策]确认登录 ID 有效，再次尝试连接。

2) HOST-198 WARNTLNT:无效的密码%

[原因]输入的密码无效。

[对策] 确认密码有效，再次尝试连接。

3) PWD-069 WARN 操作密码保护

[原因] 密码受到保护。

[对策] 请进行登录。

4) PWD-070 WARN 密码已禁用

[原因]密码已被禁用。[对策]这是密码记录。