STM32H7 系列内部存储器保护的纠错码（ECC）管理

引言

本文档介绍了 STM32H7 系列微控制器上纠错码（ECC）的管理和实现。本应用笔记针对保护内部存储器内容的 ECC 机制，描述了与之相关的硬件、软件信息。除此之外，也可使用外部存储器进行 ECC 保护，但本文档不涉及其实现方法。

本文档介绍了 ECC 保护的一般信息、详细的硬件 ECC 故障管理，以及在 STM32H7 系列微控制器中实现 ECC 的具体方法。本文档提出了安全解决方案软件部分的具体实施方法。

本文档是对参考手册 *STM32H745/755 和 STM32H747/757 高级 Arm®32 位 MCU*（RM0399）以及 *STM32H7A3/B3 高级 Arm®32 位 MCU*（RM0455）的补充，详见 www.st.com。

1 概述

下表列出了本应用笔记中使用的首字母缩略词。

表 1. 本文档中使用的缩略语

缩略语	定义
ECC	纠错码
CPU	中央处理单元（MCU 的一部分）
CRC	循环冗余校验
DED	双重错误检测
DTCM	数据紧耦合存储器
ISR	中断服务程序
ITCM	指令-紧耦合存储器
MCU	微控制器单元
MDMA	主存储器直接存取
POR	上电复位
RAM	随机存取存储器
SEC	单错误校正
SRAM	静态 RAM

STM32H7 系列微控制器是基于 Arm®的器件。

提示 *Arm 是 Arm Limited（或其子公司）在美国和/或其他地区的注册商标。*

2 ECC 概述

首个 ECC 由数学家 Richard Hamming 发明。第一个 Hamming 码使用 7 位存储 4 位信息，冗余位用于纠正和检测错误。在 STM32H7 系列器件中，RAM 和 Flash 存储器均使用基于 Hamming 原理的 SEC-DED 算法进行保护，差别在于添加了额外的奇偶校验位。ECC 码能够检测和纠正存储的数据字中的一位错误，并对两位错误进行检测。

在 SRAM 易失性存储器中，杂散的阿尔法粒子可能会导致位值翻转。这一威胁持续存在，出现一位故障的概率不会随硬件的使用年限发生改变。在大量数据长期存储而不重置的应用中（例如电池供电的数据记录器），一位或两位错误故障的问题尤为严重。

在 Flash 存储器中，数据会随时间衰减，尤其是在高温下。存储温度会对 Flash 存储器数据产生影响，但循环（编程）温度的影响更大。Flash 存储器只能对每个存储字进行一定量的重写，这就需要在数据存储的情况下实现平均抹写存储区块。特定产品 Flash 存储器的典型保留时间和生命周期详见产品数据手册。

这两种类型的故障（一位错误和两位错误）均不可避免，但正确使用 ECC 可以防止数据丢失。

表 2. 用于 SEC-DED 的额外校验位数

数据字宽	冗余位数
16	6
32	7
64	8
128	9
256	10

2.1 ECC 的影响

ECC 是嵌入式系统的关键要素之一，旨在符合安全标准的要求，如：IEC60730 C 级、IEC 61508 SIL2，乃至更高级别的标准。

缺乏硬件 ECC 的系统可能依然符合目标安全标准，但需要部署大量的软件。使用 ECC 内存能轻松地将总体诊断覆盖率提高到 90%以上，使系统能更好地符合严格的安全标准。ECC 的另一项优势是潜在的安全性改进，因为 ECC 可能会检测到硬件篡改。

2.2 RAM ECC

STM32H7 系列器件的 RAM ECC 功能具有类似外设的接口：带有设置寄存器和中断功能，能够对检测到的故障作出快速响应。所有 STM32H7x5 和 x7 SRAM 以及指令/数据高速缓存存储器均受 ECC 保护。AXI-SRAM 和 ITCM-RAM 的数据宽度为 64 位。所有其他易失性存储器均以 32 位总线宽度（字长）访问。在 STM32H7x3 上，只有紧密耦合的内存和指令/数据缓存内存受 ECC 保护，其他 SRAM 不受保护。

与普通外设的主要区别在于，RAM ECC 无法进行关闭。ECC 和 RAM 的时钟、供电同步进行，且 ECC 是 RAM 接口的组成部分。例如，禁用备份 SRAM 时，也会禁用与其关联的 RAM ECC 控制器。

ECC 根据数据字计算。如果在易失性存储器中写入了小于字的数据，则在读取-修改-写入的基础上进行修改。如果访问不完整，则 ECC 不会立即写入该值。因为当中可能涉及到紧跟的字节或半字，所以 ECC 会等待下一次写入访问。这是处理备份 SRAM 应用程序中的常见情况。例如，在字符数组中的能量守恒。但是，无法在复位的情况下完成写入操作（内存内容将被保留，且不写入最后一个不完整的字）。

对应的解决方法，是在每个常规字之后写入一个虚拟的不完整字。虚拟写入地址必须在同一内存中（本例中为备份 SRAM）。

图 1. 保留 SRAM 中的未对齐访问处理

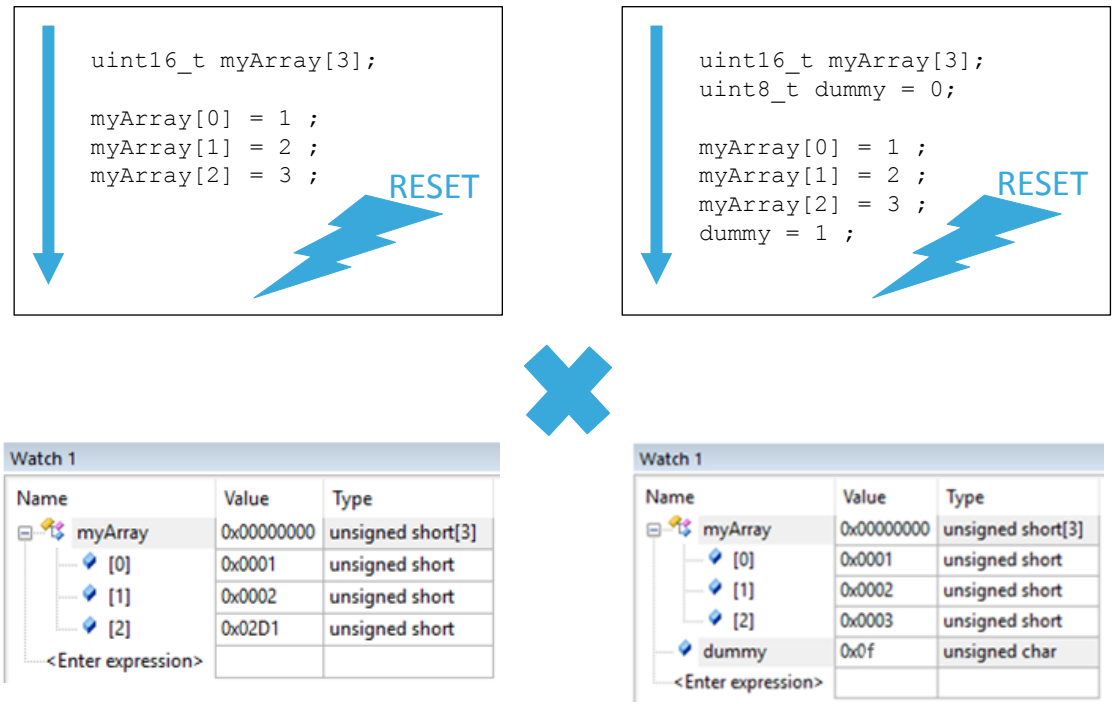
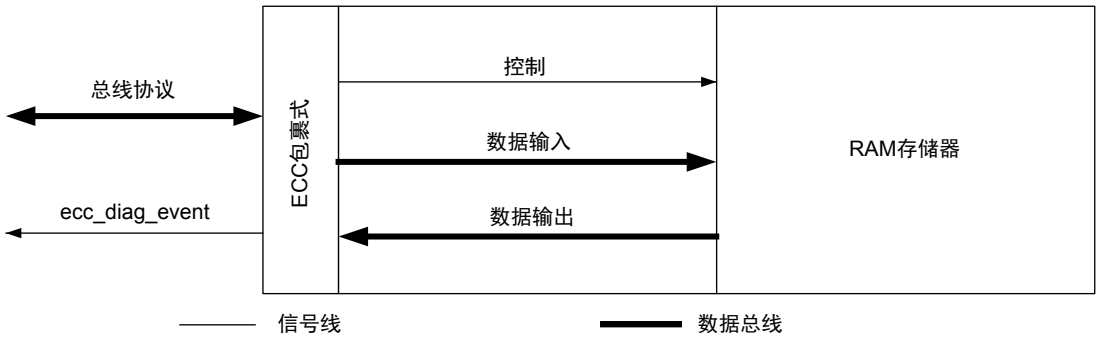
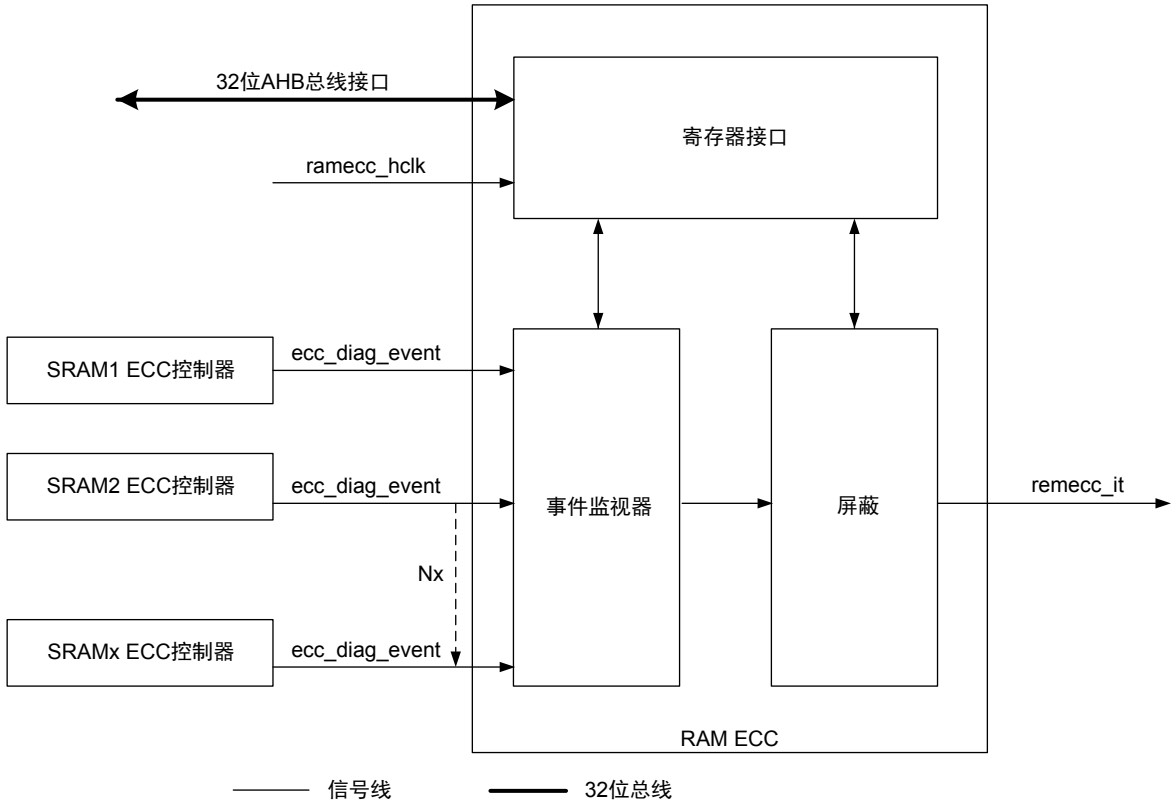


图 2. RAM ECC 控制器与内存单元接口



RAM ECC 控制器分配给每个内部 SRAM 块。控制器分为三个系统域：D1、D2 和 D3。来自所有内部 SRAM 单元/控制器的诊断信息被收集到一个全局控制块中。该全局控制块有一组配置寄存器和一个带事件可屏蔽功能的全局中断信号。

图 3. ECC RAM 简化框图



分配给特定 SRAM 块的特定 RAM ECC 控制器会在每次读取该 SRAM 块时，检查数据完整性。有些读取访问类型并不明显，因为某些写入操作包含隐式读取阶段。关于不明显的读取访问，举例来说，是在两个周期内，以读取/修改/写入的方式执行不完整 RAM 写入操作。该写入操作可以是小于 RAM 字的数据写入，也可以是未对齐写入。

2.3 Flash 存储器 ECC

对于 STM32H7x5 和 STM32H7x7 型微控制器，Flash 字（最小可编程内存量）为 256 位，而在 STM32H7x3 型上为 128 位。这也是在 Flash 字上实现 SEC 和 DED 功能所需的 10 个 ECC 位（STM32H7x3 型为 9 个 ECC 位）保护的存储器部分。只有在读取-修改-写入的基础上才能对任何较小的内存单元进行写访问，这种操作会对内存硬件造成更大的压力。STM32H7x3 型的另一个特点是在 1 千字节 OTP 区域增加了稳健性，每个 16 位都有 6 位 ECC 冗余保护。STM32H7x5 和 STM32H7x7 型上无 OTP 存储区。

ECC 功能集成在 Flash 控制器中，不能禁用。如果应用并不适用于 ECC，则可禁用相关的中断功能并忽略 Flash 状态寄存器中的标志位。

集成 ECC 解决方案的缺点在于，如果不事先擦除 Flash 字，则无法对 Flash 字中的一位进行编程。由于 EEPROM 仿真或单调计数器的实现有时使用无擦除编程，因此必须为 STM32H7 系列 MCU 上的应用选择另一种算法。

STM32H7 系列的 Flash 控制器还实现了硬件 CRC 完整性保护。CRC 能对 ECC 进行补充，但无法完全取代 ECC。如果自动后台 CRC 检查被激活，则对 Flash 存储器的读访问也会对整个范围内的 ECC 进行隐式检查。

2.4 高速缓存 ECC

缓存属于无地址范围的内存。其目的是针对频繁访问的内容（代码或数据）或未来即将需要的内容（例如，当前地址+1），通过保留此类内容的副本来减少访问寻址内存的延迟。实际上，缓存是一个具有不同寻址的 SRAM。

默认情况下，Cortex®-M7 L1 缓存也通过相同的 SEC DED 代码得到 ECC 的保护。当整个缓存行被覆盖时，字宽为 256 位。可以禁用缓存 ECC 保护。要修改缓存 ECC 的状态，首先须禁用代码并刷新缓存。然后可以修改 ECC 设置并使用新设置重新启用缓存。

CPU 缓存仅参与 AXIM 总线访问，ITCM 和 DTCM 地址范围无需缓存——紧密耦合的内存几乎专门用于 Cortex®-M7 内核。Cortex®-M7 处理器可以自动从指令缓存中检测到的任何 ECC 故障中恢复。一位错误被自动纠正覆盖。对于两位错误，该行无效，且需要再次从程序存储器中加载指令。在数据缓存的情况下，两位错误检测可能会导致在重新加载旧数据时丢失正在进行的修改。请注意，对于此类罕见事件，不建议将*透写操作*作为应对策略。

在双核 STM32H7 系列器件上支持 Cortex®-M4 内核的 ART 加速器缓存不受 ECC 保护。

由于 CPU 缓存的 ECC 检测结果缺乏故障通知或接口，针对偶发的两位数据缓存 ECC 错误，唯一解决方案是手动定期清理甚至禁用缓存。定期刷新高速缓存可防止多个失败位累积到单个高速缓存行。禁用缓存可能是极端方法，但在处理关键数据时也是一种有效的预防措施。

3 ECC 的应用

为了正确使用 ECC 功能，必须在固件中实现基本例程，以便对检测到的错误进行立即处理。建议记录并监控存在的错误，以便进行维护、故障预测和危险警告。该建议对于安全和工业应用尤为重要。

3.1 处理 RAM 中的 ECC 错误

静态易失性存储器以单极晶体管的对称排列为基础。单极晶体管在表示逻辑 0 或 1 的两种状态之间翻转。该转换过程所需的能量较低，故而可使器件保持较低的功耗。

杂散的阿尔法粒子可能会导致 RAM 中的某个位改变其存储值。如未正确使用 ECC 机制，则这些罕见的错误可能会随着时间的推移而累积并导致数据损坏甚至系统故障。

这些事件本质上是随机事件，即无法通过某些地址上发生的错误来预测下一个错误的位置或时间。

3.1.1 初始化

将 ECC 用于 RAM 时，必须对代码访问的所有存储器进行初始化。由于存储值和冗余位的随机初始设置，对未初始化存储器进行读取访问或未对齐写入，可能会触发 ECC 错误。

任何模式都适用于执行存储器初始化。以下是建议的后续步骤：

Step 1. 在 POR 或从待机模式唤醒后，或在域待机后，继续 RAM 初始化。

Step 2. 在 RAM 初始化后清除 RAM ECC 状态寄存器标志。

Step 3. 激活 ECC 错误锁存。即使是可选的，这个操作对后续错误纠正和可靠性错误也有着重要的意义。

Step 4. 使能中断，进行检测和纠错。
通过使用特定 RAM ECC 控制器单元的寄存器标志，可以选择性地仅对某些内存区域使能中断。

Step 5. 使能全局 RAM ECC 中断。

3.1.2 ECC ISR

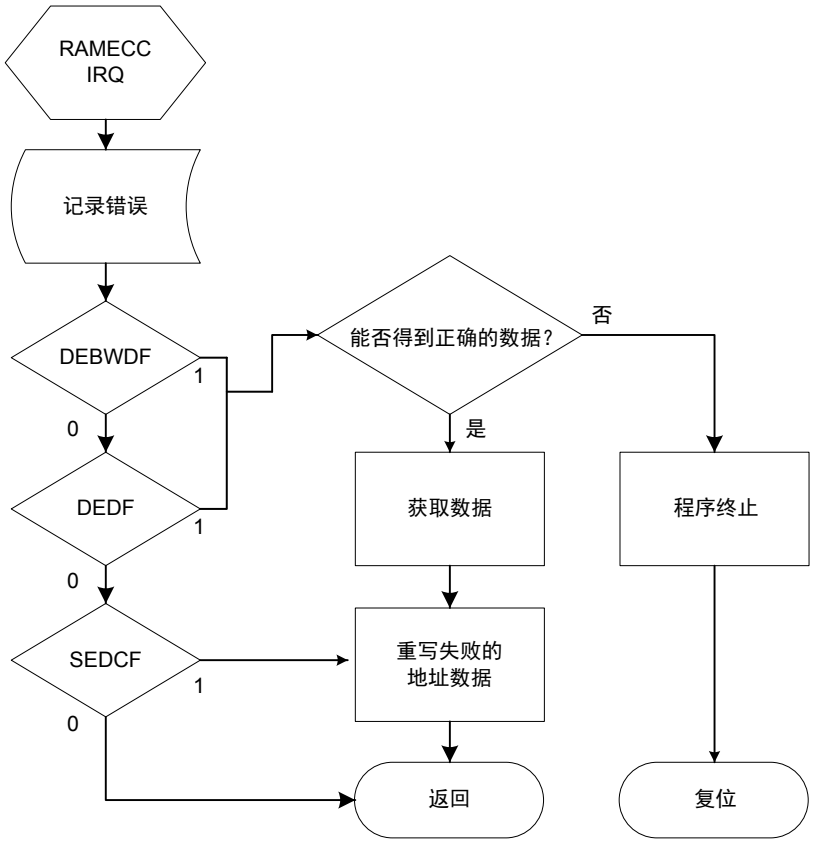
借助中断服务程序，可对 ECC 错误事件作出即时响应。然而，在 CubeHAL 中实现的 ISR（在项目中使用 STM32CubeMX 工具生成）仅仅只是一个开始。HAL ISR 分支到一个回调函数。此函数并非 HAL 的组成部分，本节提出了实现该函数的具体方法。

一位错误由 ECC 控制器自动纠正，但仅在读取数据时纠正，然后须写回修正后的数据。届时，数据和地址锁存功能将发挥重要作用。在此建议将更正后的数据写回其地址，否则可能会导致稍后出现两位故障（在同一字中的另一位损坏的情况下）。

如果仍然发生两位错误，则后续操作取决于具体损坏的内容。如果受影响的字是加载到 RAM 的代码指令，则应识别 Flash 存储器中原始代码内的加载区域，并将代码重新加载到 SRAM。同样的操作适用于任何其他初始化的部分，例如：中断向量表的副本。

如果损坏的地址落入栈区域，为了避免在不正确的上下文中执行导致进一步的损坏，必须执行系统复位。如果受影响的字地址位于数据 RAM（堆或全局变量）的边界内，则由开发人员决定，具体采取哪项操作。通常建议采取复位操作，但风险分析结论可能因情况而异。

图 4. **RAM ECC 中断动作示例**



注意：缩写是RAMECC监视器x状态寄存器中的寄存器标志（**RAMECC_MxSR**）

进行故障后操作时，可选择记录错误以便进行后续分析。

3.1.3 RAM 中 ECC 的预防措施

RAM ECC 事件具有随机性，因此可通过对已使用的 RAM 区域执行定期检查来防止损坏。通过读取每个字来激活 ECC 检查；如果检查周期合适，则可在仅有一个错误位的情况下检测到大多数错误字。适当的检查周期可以从几小时到几天不等，具体取决于外部环境中的辐射危害以及微控制器的作用。

预防性 ECC 检查无需一轮完成。此检查属于后台任务，可在空闲时刻由后台进程或低优先级 DMA 传输执行。由于 SRAM 被划分为非连续地址范围，因此不可能进行单循环或 DMA 传输。

MDMA 特别适合此任务，因其可以访问 ITCM/DTCM。使用 Cortex®-M7 CPU 进行内存读取检查时，会涉及到缓存（前提是已启用缓存）。通过 Cortex®-M7 缓存访问 SRAM（ITCM 和 DTCM 不在此规则中），从内存中读取的每个数据都会填充 256 位的缓存行。激活每个内存字 ECC 检查的循环只读取每个 256 位的第一个字，并由缓存行继续加载剩余的字。此操作会降低 CPU 负载，但总线仍会保持高负载。

3.2 处理 Flash 存储器中的 ECC 错误

Flash 存储器的典型故障是由于存储单元抹写导致的故障和电荷泄漏导致的故障。相邻单元的干扰或编程期间的电压不稳定也可能导致故障。与 SRAM 不同，特定 Flash 存储器地址中的故障可能表明同一页中发生后续故障的可能性略高。新器件上不应存在 Flash 存储器错误，故障概率会在预计寿命结束时增加。Flash 存储器的寿命主要取决于温度条件和擦除周期。

3.2.1 Flash 存储器 ECC ISR

对于 Flash 存储器，ECC 错误通知中断包含在 Flash 存储器全局中断向量中。ISR 检查 Flash 状态寄存器 Flash_SR1 的 ECC 标志“单次纠错”和“双重错误检测”，并采取适当的措施（取决于 Flash 存储器的用途）。由于中断向量与正常 Flash 存储器操作共享（如“编程结束”），ISR 应将控制权传递给 HAL，以处理其他标志。

3.2.2 Flash 存储器代码

片上非易失性存储器主要用于代码。正常情况下，代码的重写频率不高，因此如果发生损坏，很可能是由于老化和电荷泄漏。在双区器件上，可以拥有相同代码的第二副本，并在指示 ECC 错误时交换到该第二副本。该解决方案意味着监控两个存储区内容的健康状况。可通过健康的存储区对另一个存储区的不合格内容进行重新编程，但是不能保证此操作可以有效提高器件的预期寿命。

3.2.3 EEPROM 仿真

如果故障 Flash 存储器单元用于存储数据，则故障原因可能与程序/擦除循环有关。在高级 EEPROM 仿真实现中，包含了处理故障存储单元并将其排除在循环之外的机制。

3.2.4 Flash 存储器中 ECC 的预防措施

CRC 硬件模块能够有效监控嵌入式 Flash 存储器的运行状况。CRC 可自动检查整个存储区或特定地址范围；ECC 也会在读取时进行隐式检查。然后，程序必须对检测到的问题作出响应。

4 结论

随着微电子技术在系统中的集成度越来越高，存储单元较易发生故障，因此 ECC 存储器完整性保护变得愈加重要。RAM ECC 与常规外设之间的主要区别在于——RAM ECC 作为 RAM 接口组成部分，无法进行关闭。

本应用笔记对 RAM、Flash 存储器和高速缓存中的 ECC 进行了介绍，

此外还提供了处理 RAM 和 Flash 中 ECC 错误的程序。

版本历史

表 3. 文档版本历史

日期	版本	变更
2019 年 5 月 27 日	1	初始版本。
2020 年 1 月 6 日	2	更新了： • 第 引言 • 第 2.2 节 RAM ECC • 第 2.3 节 Flash 存储器 ECC

目录

表一览

图一览