LabMES 与 PLC 通信接口说明书

西门子 S7 非优化 DB 布局 · 基于 UDT_MES V0.1 · 文档版本 1.0

1. 概述

本说明书定义 LabMES 制造执行系统与西门子 PLC 之间的数据交互规范。采用 **S7 非优化数据块（DB）**，所有多字节数值均为**大端序（Big-Endian）**。字符串使用 Siemens `STRING[n]` 格式，占 `n+2` 字节（首字节为最大长度，第二字节为当前长度）。

数据块总长度 **2981 字节**，`End` 位于偏移 2980。PLC 端通过 `RequestCmd` 发起命令，MES 端通过 `Done` 和业务回写区反馈结果。通信基于轮询机制，Worker 每 150 ms 检测命令与报警。

> **重要：**仓库内的 `plc/UDT_MES.udt` 和 `plc/MES.db` 为旧版导出文件，现场部署前应替换为新版导出。字段扩展或 PLC DB 变化时，必须同步核对偏移和总长度。

2. DB 字节布局

下表列出 `UDT_MES` 结构体的完整字节偏移、长度及数据类型。数组元素按元素偏移递增计算，详见 2.1 数组地址计算。

字段	起始偏移	长度(字节)	数据类型 / 说明
`RequestCmd`	0	2	Int，PLC 命令码。0=空闲，1=SN过站校验，2=上传生产数据，3=托盘过站校验，4=产品返工，5=产品打印，6=托盘查询SN，7=SN查询托盘，0x0A=查询配方

字段	起始偏移	长度(字节)	数据类型 / 说明
`Alarm[1..800]`	2	100	Bool 数组，DBB2..DBB101。PLC 报警位，索引说明见 `plc/alarm/{设备}.csv`
`StationId`	102	22	STRING[20]，工位 ID（PLC 填写）
`WpcNumberId`	124	22	STRING[20]，托盘号（PLC 填写或 MES 回写）
`SerialNumber`	146	52	STRING[50]，产品序列号（PLC 填写或 MES 回写）
`Status.Result`	198	2	Int，结果判定：0=MES综合判断，1=PLC判断Passed，2=PLC判断Failed
`Status.StartTime`	200	22	STRING[20]，开始时间（从 DateTime 复制）
`Status.EndTime`	222	22	STRING[20]，结束时间（从 DateTime 复制）
`Status.CT`	244	2	Int，循环时间：0=MES综合计算，其他=PLC_CT值
`ProcessData[1..40]`	246	240	每项 6 字节：id(Int) + Value(Real)。id≠0 时上传
`LimitTest[1..40]`	486	640	每项 16 字节：ID(Int), Max(Real), Min(Real), Value(Real), Result(Int)。ID≠0 时上传
`PartCode[1..10]`	1126	540	每项 54 字节：ID(Int) + Code(STRING[50])。ID≠0 时上传
`Done`	1666	2	Int，MES 状态：0=空闲，1=Busy，2=Done，3=Error。PLC 不得写入
`DateTime`	1668	22	STRING[20]，MES 下发时间，供 PLC 超时报警及 Start/EndTime 复制
`ErrorId`	1690	2	Word，MES 下发错误代码，HMI 显示用
`ErrorMessage`	1692	254	STRING[252]，MES 下发错误内容，HMI 显示用

字段	起始偏移	长度(字节)	数据类型 / 说明
`IsWork`	1946	2	Int，过站检查状态（MES 下发）
`ProductStatus`	1948	52	STRING[50]，产品最新状态（MES 下发）
`ProductStation`	2000	22	STRING[20]，产品最新位置（MES 下发）
`OrderNumber`	2022	22	STRING[20]，订单号（MES 下发，用于 Cmd=1/3）
`ProductName`	2044	22	STRING[20]，产品名称（MES 下发，用于 Cmd=1/3）
`WpcNumberId` (回写)	2066	22	STRING[20]，MES 回写托盘号（用于 Cmd=7）
`SerialNumber` (回写)	2088	52	STRING[50]，MES 回写序列号（用于 Cmd=6）
`RecipeReal[1..50]`	2140	300	每项 6 字节：id(Int) + Value(Real)。查询配方回写用
`RecipeString[1..10]`	2440	540	每项 54 字节：ID(Int) + Value(STRING[50])。查询配方回写用
`End`	2980	1	Byte，尾部占位，不参与业务判断

2.1 数组地址计算

数组元素按元素偏移递增，计算公式如下（i 从 1 开始）：

- `ProcessData[i] = 246 + (i-1) * 6`
- `LimitTest[i] = 486 + (i-1) * 16`
- `PartCode[i] = 1126 + (i-1) * 54`
- `RecipeReal[i] = 2140 + (i-1) * 6`

- `RecipeString[i] = 2440 + (i-1) * 54`

> **批量写入**：对于 `RequestCmd=0x01/0x03`，MES 结果从 DBB1946 起连续一次写入 194 字节（DBB1946..DBB2139），包含 IsWork、ProductStatus、ProductStation、OrderNumber、ProductName、WpcNumberId 和 SerialNumber。

3. 命令与握手

`RequestCmd` 位于 DBB0..DBB1（大端 Int）。非零命令读取 DBB0 起始数据：`0x02` 读取 1666 字节（DBB0..DBB1665），其他命令读取 198 字节。命令输入字段为 `StationId` (DBB102)、`WpcNumberId` (DBB124) 和 `SerialNumber` (DBB146)。

RequestCmd	业务	输入字段	MES 执行
0x00	空闲	无	写 `Done=0` 并更新时间到 `DateTime`
0x01	SN 过站校验	SerialNumber, StationId	执行 `sp_SerialNumberCheck`，成功则一次写入过站结果（DBB1946..DBB2139），最后写 `Done=2`
0x02	上传生产数据	StationId, WpcNumberId, SerialNumber, Status, ProcessData, LimitTest, PartCode	同一事务写入 Station/ProcessCode/ProcessData/LimitData，成功写 `Done=2`，失败写 `Done=3`
0x03	托盘过站校验	WpcNumberId, StationId	执行 `sp_WpcNumberIdCheck`，成功则一次写入过站结果，最后写 `Done=2`
0x04	产品返工	SerialNumber, StationId	执行 `sp_SerialNumberRework`，成功不写业务结果字段，只写 `Done=2`

RequestCmd	业务	输入字段	MES 执行
0x05	产品打印	SerialNumber, StationId	执行 `sp_SerialNumberPrint`，成功不写业务结果字段，只写 `Done=2`
0x06	托盘查询 SN	WpcNumberId	执行 `sp_SelectWpcNumberIdSn`，必须返回非空 SN，写入回写区 SerialNumber (DBB2088)
0x07	SN 查询托盘	SerialNumber	执行 `sp_SelectSnWpcNumberId`，必须返回非空托盘号，写入回写区 WpcNumberId (DBB2066)
0x0A	查询配方	StationId, SerialNumber, WpcNumberId	执行 `sp_SelectRecipe`，序列号/托盘号为空传 NULL。分别连续写入 RecipeReal (DBB2140, 300字节) 和 RecipeString (DBB2440, 540字节)，成功后写 `Done=2`

3.1 单次命令处理顺序

1. Worker 每 150 ms 轮询命令和报警。只有检测到 `RequestCmd` 从 0 变为非零才创建新事件；持续非零不会重复执行。启动时若命令已非零，只同步状态，等 PLC 清零后才接受下一条。
2. 检测到新命令后读取对应长度的数据，并先写 `Done=1` 表示处理中。
3. 按上表执行 SQL 存储过程或上传事务。`0x01/0x03/0x06/0x07/0x0A` 先写业务结果字段，再写最终 Done；`0x02/0x04/0x05` 成功时直接写最终 Done。
4. 成功写 `Done=2`。业务处理失败时，先写 `ErrorId=1` 和 `ErrorMessage`，再写 `Done=3`。`0x06/0x07` 未返回必需的 SN/托盘号也按失败处理。
5. PLC 读取终态后清零 `RequestCmd` 并清理业务输入字段；PLC 不得写 `Done`，也不得清除持续状态的 `Alarm`。

> **注意：**当前 Worker 未实现超时后写 `Done=0xFF` 的逻辑；`Done=0xFF` 仅为协议预留值。PLC 通信中断或写入失败时，Worker 会

> 记录错误并尝试重连，不能保证写入终态。

4. 数据上传规则（RequestCmd=0x02）

一次读取 DB 起始地址 0、长度 1666 字节（DBB0..DBB1665，覆盖上传所需的 PartCode 数组，不读取 Done 及其后的 MES 区域）。以下记录应放在**同一个 SQL 事务**中，任一操作失败即回滚并返回 `Done=3`。

目标表	来源与规则
`dbo.Station`	通过 `sp_InsertStatus` 写入工位、托盘、SN、结果、起止时间和 CT；PLC 调用不传 orderid、productid
`dbo.ProcessCode`	`PartCode` 中 `ID ≠ 0` 的项；用 `plc/Variable.csv` 将 ID 映射为物料名称
`dbo.ProcessData`	`ProcessData` 中 `id ≠ 0` 的项；映射变量名、单位和值
`dbo.LimitData`	`LimitTest` 中 `ID ≠ 0` 的项；映射变量名、单位、实测值、上下限和结果

`sp_InsertStatus` 使用参数化执行，并与后续批量写入共用同一 SQL 事务；数组项按批量参数化 INSERT 写入，未使用项以 ID 为 0 跳过。

`LimitTest.Result` 取值：`0` = 按上下限判断，`1` = Passed，`2` = Failed。`Status.Result=0` 时依据有效限值结果判定；无有效项时不判定。写入 SQL 的结果使用字符串，不写 PLC 的数值枚举。

5. 查询配方（RequestCmd=0x0A）

存储过程 `sp_SelectRecipe @station, @SerialNumber, @WpcNumberId` 返回 JSON 格式反馈：

```
{
  "RecipeReal": [
    {"vid": 1001, "value": "100"},
    {"vid": 1002, "value": "100"}
  ],
  "RecipeString": [
    {"vid": 1003, "value": "ABCD"}
  ]
}
```

`vid` 写入 PLC 数组元素的 `id:Int` 字段，不用作数组索引；PLC 槽位按过程返回数组的顺序排列，不要求 VID 连续或唯一。只检查数组条目数不超过 `RecipeReal` 的 50 项和 `RecipeString` 的 10 项，并要求 ID 可编码为 PLC Int。未返回的槽位清零。

MES 分别连续写入 `RecipeReal`（DBB2140，300 字节）和 `RecipeString`（DBB2440，540 字节），两次写入成功后写 `Done=2`，不执行写后回读。反馈数组缺失、数组超限、ID 无法编码、Real 无效或字符串超过 50 字符时按业务失败处理并写 `Done=3`。

6. 报警处理

报警数组 `Alarm[1..800]` 每轮比较前后状态：

- `0→1`：新增报警记录（向 `dbo.Alarm` 执行 INSERT）
- `1→0`：关闭未解除记录（向 `dbo.Alarm` 执行 UPDATE）

报警索引及说明从 `plc/alarm/{设备名称}.csv` 读取。PLC 不得清除持续状态的 `Alarm`。

7. 设备服务与日志

PLC 配置位于 `plc/Driver.json`，每台设备配置 `Name`、`Tppe`、`PlcIP`、`rack`、`slot`、`DB`。服务采用每设备一个 Worker 的模型，设备之间独立轮询、重连和记录状态；同一设备不并发发起读取。

`RequestCmd=2` 读取 1666 字节（DBB0..DBB1665），其他非零命令读取 198 字节（DBB0..DBB197）；Done 为 2 字节 Int，DateTime、错误区和 MES 回写区分别按偏移表读写。

设备状态包含连接状态、心跳、命令、Done、CT、产品信息和最近错误。Request 日志按本次实际读取长度显示完整 DB 变量名及解析值，不显示未读取区域的补零数据，也不展开占用较多日志空间的 `Alarm` 数组：普通命令显示 DBB0..DBB197 内其他变量，上传命令显示 DBB0..DBB1665 内其他变量。`ProcessData.id`、`LimitTest.ID`、`PartCode.ID` 为 0 的数组占位项不写入日志；PLC 上传和报警边沿日志不受此过滤影响。

通信日志还应保留 SQL 参数/结果、PLC 应答及耗时；SQL 执行失败时将失败语句合并到 `SQL 业务处理失败` 记录，例如 `executePrint;SQL 业务处理失败;{EXEC sp_InsertStatus ...}`；Done 写入按实际 Int 值记录，例如 `writePlc;DB5001,C1666.2;value=3;`。

> **页面数据来源：**普通页面从服务端状态缓存读取，不直接连接 PLC。

8. 数据类型与字节序

类型	长度	说明
Int	2 字节	有符号整数，大端序
Word	2 字节	无符号整数，大端序
Real	4 字节	IEEE 754 浮点数，大端序
Bool	1 位	按位打包，Alarm 数组每 8 位占 1 字节
STRING[n]	n+2 字节	首字节最大长度，第二字节当前长度，后续为字符内容

9. 附录：命令与反馈速查

0x01 / 0x03 过站校验反馈格式

```
{
  "IsWork": ...,
  "ProductStatus": "...",
  "ProductStation": "...",
  "OrderNumber": "...",
  "ProductName": "...",
  "WpcNumberId": "...",
  "SerialNumber": "..."
}
```

MES 从 DBB1946 一次连续写入 194 字节（DBB1946..DBB2139），随后写 `Done=2`。

0x06 / 0x07 查询反馈

- `0x06`：`sp_SelectWpcNumberIdSn` 返回非空 SN，写入 DBB2088（STRING[50]）
- `0x07`：`sp_SelectSnWpcNumberId` 返回非空托盘号，写入 DBB2066（STRING[20]）

0x02 上传数据字段有效性

- `ProcessData`：`id ≠ 0` 的项上传
- `LimitTest`：`ID ≠ 0` 的项上传
- `PartCode`：`ID ≠ 0` 的项上传
- 未使用项以 ID 为 0 跳过

LabMES 制造执行系统 · PLC 通信接口说明书 · 基于 UDT_MES V0.1 · 文档生成日期 2025-03-21