**Zeno G3-PLC 自动注册功能设计说明**

# **G3-PLC电表系统注册**

PLC表计注册、网络维护和心跳机制等，在PLC通信中自动完成，相关工作机制的细节描述参考章节4.2。

PLC表计注册过程（以G3-PLC为例）：

1. 在系统同时上电后，表计从模块随机延时0~300秒，提交注册申请到集中器（在G3-PLC组网路由过程中，优先按照预置频段寻找信号最优的主节点） 。
2. 如果该表计未列入集中器的子表白名单，则集中器将拒绝注册申请，并推送事件信息到前置机。
3. 前置机收到新表注册申请后，根据不同情况做出反馈：
   1. 如果该表计还未在任何集中器注册，则允许表计注册到该集中器；更新白名单，配置密钥等参数（用“新增”方式追补白名单，不复位主模块）。待该表计再次提出申请时，顺利入网。
   2. 如果该表计曾经注册过其它集中器，并且上次注册时间与本次新申请时间的间隔小于1天，则拒绝以防止在集中器之间频繁切换。
   3. 如果该表计曾经注册过其它集中器，但两次注册时间间隔大于1天，则允许表计注册到该集中器，同时更新两台集中器的白名单。（该机制主要用于G3-PLC网络优化）
4. 表计在第一次申请注册后，因为不在集中器白名单中，因而被拒绝。在延时5分钟之后，表计将发起第二次注册申请到同一集中器。如果被连续拒绝3次，则尝试向其它集中器发起申请，轮询完所有集中器后；再顺次切换其它频段（CenA -> FCC -> FCCH），直到注册成功。
5. 表计完成注册后，记忆从属的主集中器和工作频段，在下次上电后自动寻找主集中器、按存储工作频段入网。
6. 在网运行过程中，G3-PLC网络采取以下维护机制：
   1. 从模块将按30分钟间隔发起心跳检测，期待主模块回应。如连续4次心跳没有回应（120分钟），则判定为网络异常。
   2. 从模块与主模块定期通信，如连续90分钟无通信活动，则判定该从模块“暂时失联”，使集中器不再抄读该从模块所在的表计；如果主模块再次收到该从模块的心跳，则清除“暂时失联”状态，使下次集中器可正常抄读该从模块所在的表计。

从模块满足上述条件a)，判定为异常后，将自动恢复到新表注册状态，重复执行上述A~E步骤。

*网络异常的可能原因有：集中器变更了白名单、移除子表、通信链路中断或更改了 GMK 通信密钥等。*

# G3-PLC模块注册

PLC的路由组网和注册由主模块管理，按以下方式工作。

主模块（上文名称为G3-PLC主节点）：

* 作为独立组件，安装在集中器、Gateway等主机中。
* 提供主机管理接口，以配置白名单、注册模式、路由表等工作参数和数据。
* 上电后，从主机获取子模块白名单；并总是基于白名单工作。
* 如果申请入网的子模块不在白名单中，则拒绝入网，并将注册申请推送到主机（根据配置）。
* 如主机允许新的子模块入网，则更新表计档案到模块主机，同步更新主模块白名单；等待子模块的下一轮入网申请。

从模块（上文名称为G3-PLC从节点）：

* 上电后自动读取表计序号，向主模块发送入网请求。
* G3-PLC规范有 CenA/FCC/FCCH 上个工作频段，在发起MAC/PHY层通信之前，需要根据预置参数，配置好频段参数，并初始化。
  + 频段参数默认为FCC 以获得最优的通信性能和最大的适用范围。
  + 可在出厂前或现场修改频段参数，并存储到外部 FLASH。
  + 上电后优先寻找预置频段，如入网失败，则依次切换其它频段尝试。（自动切换频段功能有两个问题：一是造成入围效率降低，耗时过长；二是由于MAC/PHY层在运行过程中的时序不一致，产生问题。）
* 等待主模块响应，如拒绝入网，则主模块将提交新表注册信息到集中器，等待系统审批。（自动注册功能可关闭）
* 从模块记忆注册状态（集中器、工作频段），如掉电后再次上电，优先登录已注册的集中器；如果不能正常连接，再按照信号强弱依次寻找其它集中器。
* 在第一次被主模块拒绝后，从模块将延时5分钟后重新注册，连续5次失败后，尝试其它主模块；或最大间隔30分钟后，启动下一轮注册申请。
* 每30分钟发送心跳给集中器，如果连续丢失4个心跳，则重新发起入网请求；或连续90分钟未与主模块通信，则主模块将该从模块置为“失联状态”。该功能主要用于集中器档案变更、拆除替换或子表变更主机；前置机配合做集中器变更注册功能。

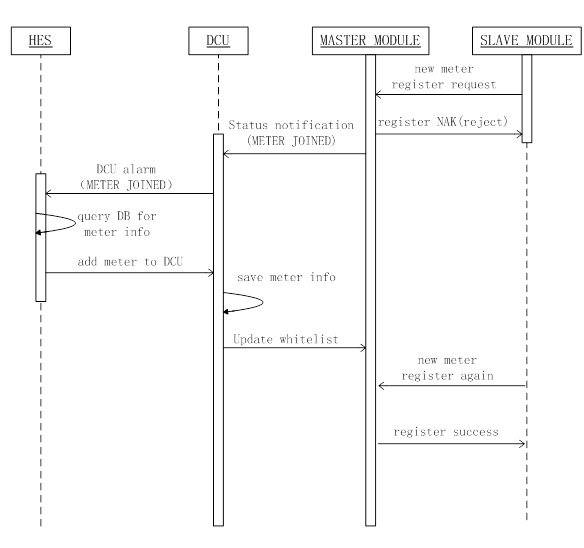
集中器或Gateway：

* 前置机可以启用或关闭自动注册功能。
* 上电或运行过程中，分析子表档案信息，更新白名单到主模块。
* 如接收到来自主模块的申请注册消息，则推动给前置机。
* 集中器收到来自前置机的确认信息，更新子表档案信息，并更新白名单到主模块。

前置机：

* 前置机将从集中器检测表计的注册请求。
* 如果确认新表可以接受，则更新表计信息（通信密钥，安全等级等）。
* 如果收到的注册信息是其它集中器已注册过的，且相关集中器未更换、拆除、故障等，则忽略请求。
* 可手工调整子表档案配置。

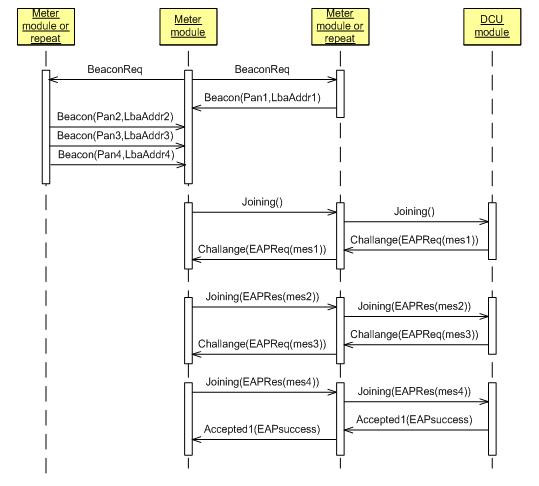
工作流：



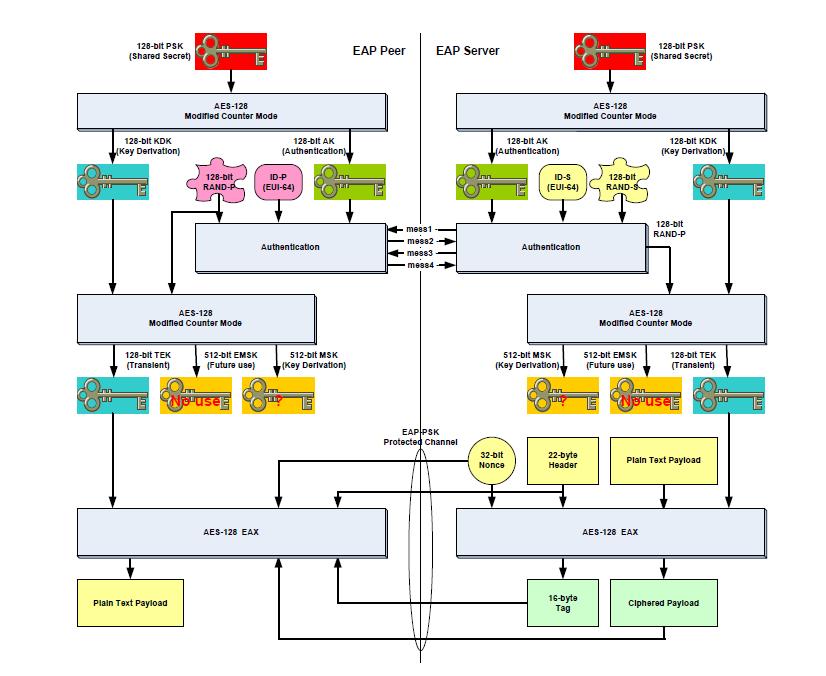
# G3-PLC通信加密

EAP-PSK加密认证方案

如果要用到PSK对电表进行入网加密认证，一个有效的表档案必须包括表的serial number与电表的PSK。集成商或客户在电表出厂前，就要把这两个参数告诉电表生产厂家，电表在出厂前，这两个参数被预先设置到电表中。电表PLC模块从电表上读取这两个值，并携带这两个值去向集中器模块发起入网注册申请。集中器模块中如已保存这块表的档案(档案中必须包含电表的serial number与电表的PSK)，将会对这块表进行双向加密认证，下面是电表模块加入PLC网络流程图：



上图中入网认证需要交互的mes1,mes2,mes3,mes4产生流程图如下：



上图的EAP Peer对应我们的电表模块，EAP Server 对应我们的集中器模块。

由于PSK与电表serial number 是成对出现的，是入网认证过程的必备材料，因此PSK也应该保存在电表上，保持与模块无关。现场更换模块，将不需要重设PSK。