OBJETO

El presente documento tiene como objetivo proporcionar unas pautas seguras de codificación de PLC. Trata de una lista con las 20 prácticas seguras principales.

PRÁCTICAS SEGURAS DE CODIFICACIÓN DE PLC: LISTA DE LAS 20 PRINCIPALES

1. **Modularizar el código del PLC**
   Dividir el código PLC en módulos, utilizando diferentes bloques de funciones (subrutinas). Probar los módulos de forma independiente.

2. **Seguir los modos operativos**
   Mantener el PLC en modo RUN. Si los PLC no están en modo RUN, debe haber una alarma para los operadores.

3. **Dejar la lógica operativa en el PLC siempre que sea posible**
   Dejar la mayor parte de la lógica operativa, por ejemplo, la totalización o la integración, directamente en el PLC. La HMI no recibe suficientes actualizaciones para hacerlo bien.

4. **Utilizar indicadores de PLC como comprobaciones de integridad**
   Poner contadores en los indicadores de error del PLC para capturar cualquier problema matemático.

5. **Realizar comprobaciones de integridad criptográficas y/o de suma de comprobación para el código PLC**
   Utilizar hashes criptográficos, o sumas de comprobación si los hashes criptográficos no están disponibles, para comprobar la integridad del código del PLC y emitir una alarma cuando cambien.

6. **Validar temporizadores y contadores**
   Si los valores de los temporizadores y contadores se escriben en el programa del PLC, el PLC debe validarlos para verificar que sean razonables y verificar los recuentos hacia atrás por debajo de cero.

7. **Validar y alertar sobre entradas/salidas emparejadas**
   Si tiene señales emparejadas, asegúrese de que ambas señales no se afirmen juntas. Alarma al operador cuando ocurren estados de entradas/salida que no son físicamente factibles. Considere la posibilidad de independizar las señales emparejadas o de añadir temporizadores de retardo cuando la conmutación de las salidas pueda ser perjudicial para los actuadores.

8. **Validar las variables de entrada de HMI en el nivel del PLC, no sólo en la HMI**
   El acceso de la HMI a las variables del PLC puede (y debe) restringirse a un rango de valores operativos válidos en la HMI, pero deben añadirse otras comprobaciones cruzadas en el PLC para evitar, o alertar sobre, valores fuera de los rangos aceptables que están programados en la HMI.

9. **Validar indirecciones**
   Valide las indirecciones envenenando los extremos de la matriz para detectar errores en los postes de la cerca.

10. Asignar bloques de registro designados por función (lectura/escritura/validación)

Asigne bloques de registro designados para funciones específicas con el fin de validar los datos, evitar el desbordamiento del búfer y bloquear las escrituras externas no autorizadas para proteger los datos del controlador.

11. Instrumentar el control de plausibilidad

Instrumentar el proceso de forma que permita comprobar la verosimilitud mediante la comprobación cruzada de diferentes mediciones.

12. Validar entradas basadas en plausibilidad física

Asegúrese de que los operadores sólo pueden introducir lo que es práctico o físicamente factible en el proceso. Establezca un temporizador para una operación con la duración que debe tener físicamente. Considere alertar cuando haya desviaciones. Avise también cuando hay una inactividad inesperada.

13. Desactivar los puertos y protocolos de comunicación innecesarios/no utilizados

Los controladores del PLC y los módulos de interfaz de red soportan, generalmente, varios protocolos de comunicación que están activados por defecto. Desactive los puertos y protocolos que no sean necesarios para la aplicación.

14. Restringir las interfaces de datos de terceros

Restrinja el tipo de conexiones y los datos disponibles para interfaces de terceros.
Las conexiones y/o interfaces de datos deben estar bien definidas y restringidas para permitir únicamente la capacidad de lectura/escritura para la transferencia de datos requerida.

15. Definir un estado de proceso seguro en caso de reinicio del PLC

Definir estados seguros para el proceso en caso de reinicio del PLC (por ejemplo, energizar los contactos, desenergizar, mantener el estado anterior).

16. Resumir los tiempos del ciclo del PLC y su tendencia en la HMI

Resuma el tiempo de ciclo del PLC cada 2-3 segundos e informe a la HMI para visualizarlo en un gráfico.

17. Registre el tiempo de actividad del PLC y su tendencia en la HMI

Registre el tiempo de actividad del PLC para saber cuándo se reinició. Tendencia y registro del tiempo de actividad en la HMI para el diagnóstico.

18. Registrar las paradas duras del PLC y realice la tendencia de ellas en la HMI

Almacena los eventos de parada dura del PLC por fallos o apagados para que los sistemas de alarma de la HMI los consulten antes de reiniciar el PLC. Sincronización horaria para obtener datos más precisos.

19. Supervisar el uso de la memoria del PLC y su tendencia en la HMI

Medir y proporcionar una línea de base para el uso de la memoria para cada controlador desplegado en el entorno de producción y tendencia en la HMI.

20. Programar trampa de falsos negativos y falsos positivos para alertas críticas

Identificar las alertas críticas y programar una trampa para esas alertas. Configure la trampa para supervisar las condiciones de activación y el estado de alerta para cualquier desviación.