



OBJECTE

Aquest document té com a objectiu proporcionar unes pautes segures de codificació de PLC. És una llista amb les 20 pràctiques segures principals.

PRÀCTIQUES SEGURES DE CODIFICACIÓ DE PLC: LLISTA DE LES 20 PRINCIPALS

1. Modularitzar el codi del PLC

Dividir el codi PLC en mòduls, utilitzant diferents blocs de funcions (subrutines). Provar els mòduls de manera independent.

2. Seguir els modes operatius

Mantenir el PLC en mode RUN. Si els PLC no estan en mode RUN, ha d'haver-hi una alarma per als operadors.

3. Deixar la lògica operativa en el PLC sempre que sigui possible

Deixar la major part de la lògica operativa, per exemple, la totalització o la integració, directament en el PLC. L'HMI no rep prou actualitzacions per fer-ho bé.

4. Utilitzar indicadors de PLC com a comprovacions d'integritat

Posar comptadors en els indicadors d'error del PLC per capturar qualsevol problema matemàtic.

5. Fer comprovacions d'integritat criptogràfiques i/o de suma de comprovació per al codi PLC

Utilitzar empremtes electròniques, o sumes de comprovació si les empremtes electròniques no estan disponibles, per comprovar la integritat del codi del PLC i emetre una alarma quan canviïn.

6. Validar temporitzadors i comptadors

Si els valors dels temporitzadors i comptadors s'escriuen al programa del PLC, el PLC ha de validar-los per verificar que siguin raonables i verificar els recomptes cap enrere per sota de zero.

7. Validar i alertar sobre entrades/sortides aparellades

Si teniu senyals aparellats, assegureu-vos que ambdós senyals no s'afirmen junts. Alarma l'operador quan ocorren estats d'entrades/sortides que no són físicament factibles. Considereu la possibilitat d'independitzar els senyals aparellats o d'afegir-hi temporitzadors de retard quan la commutació de les sortides pugui ser perjudicial per als actuadors.

8. Validar les variables d'entrada d'HMI en el nivell del PLC, no només en l'HMI

L'accés de l'HMI a les variables del PLC pot restringir-se (i cal fer-ho) a un rang de valors operatius vàlids en l'HMI, però han d'afegir-se altres comprovacions creuades en el PLC per evitar, o alertar sobre, valors fora dels rangs acceptables que estan programats en l'HMI.

9. Validar indireccions

Valideu les indireccions enverinant els extrems de la matriu per detectar errors en els pals de la tanca.

10. Assignar blocs de registre designats per funció (lectura/escriptura/validació)



Assigneu blocs de registre designats per a funcions específiques amb la finalitat de validar les dades, evitar el desbordament del "buffer" i bloquejar les escriptures externes no autoritzades per protegir les dades del controlador.

11. Instrumentar el control de plausibilitat

Instrumentar el procés de manera que permeti comprovar la versemblança mitjançant la comprovació creuada de diferents mesuraments.

12. Validar entrades basades en plausibilitat física

Assegureu-vos que els operadors només poden introduir el que és pràctic o físicament factible en el procés. Establiu un temporitzador per a una operació amb la durada que ha de tenir físicament. Considereu alertar quan hi hagi desviacions. Aviseu també quan hi ha una inactivitat inesperada.

13. Desactivar els ports i protocols de comunicació innecessaris / no utilitzats

Els controladors del PLC i els mòduls d'interfície de xarxa admeten, generalment, diversos protocols de comunicació que estan activats per defecte. Desactiveu els ports i protocols que no siguin necessaris per a l'aplicació.

14. Restringir les interfícies de dades de tercers

Restringiu el tipus de connexions i les dades disponibles per a interfícies de tercers. Les connexions i/o interfícies de dades han d'estar ben definides i restringides per permetre únicament la capacitat de lectura/escriptura per a la transferència de dades requerida.

15. Definir un estat de procés segur en cas de reinici del PLC

Definir estats segurs per al procés en cas de reinici del PLC (per exemple, energitzar els contactes, desenergitzar-los, mantenir l'estat anterior).

16. Resumir els temps del cicle del PLC i la seva tendència en l'HMI

Resumiu el temps de cicle del PLC cada 2-3 segons i informeu l'HMI per visualitzar-lo en un gràfic.

17. Registrar el temps d'activitat del PLC i la seva tendència en l'HMI

Registreu el temps d'activitat del PLC per saber quan es va reiniciar. Tendència i registre del temps d'activitat en l'HMI per al diagnòstic.

18. Registrar les parades dures del PLC i realitzar-ne la tendència en l'HMI

Emmagatzema els esdeveniments de parada dura del PLC per fallades o apagades perquè els sistemes d'alarma de l'HMI els consultin abans de reiniciar el PLC. Sincronització horària per obtenir dades més precises.

19. Supervisar l'ús de la memòria del PLC i la seva tendència en l'HMI

Mesurar i proporcionar una línia de base per a l'ús de la memòria per a cada controlador desplegat a l'entorn de producció i tendència en l'HMI.

20. Programar parany de falsos negatius i falsos positius per alertes crítiques

Identificar les alertes crítiques i programar un parany per a aquestes alertes. Configureu el parany per supervisar les condicions d'activació i l'estat d'alerta per a qualsevol desviació.

