CURSO: PROGRAMACIÓN DE CONTROLADORES Y LOCALIZACIÓN DE FALLAS EN MECATRÓNICA

Video 03 — Parte 2A: Detección de Fallas, Temporizador Vigilante (Watchdog), Paridad y Codificación de Errores — Confiabilidad MTBF/MTTF, Redundancia, FMEA/FTA, Watchdog de Ventana, Paridad LRC, Checksum, CRC-16/32 y Código Hamming SECDED

Parte del Curso: Parte 2A (Tema 5A) — Detección de Fallas, Temporizador Vigilante (Watchdog), Paridad y Codificación de Errores
Enfoque de Programación y Diagnóstico: Confiabilidad MTBF/MTTF, Redundancia 2oo3 y Analítica, FMEA/FTA, Windowed Watchdog con Banderas de Latido, Paridad LRC, CRC-16/32 y Código Hamming SECDED

```
NPR = S × O × D | Residuo: r[k] = y[k] - y_hat[k] | Ventana WWDG: T_min < t_kick < T_max | Síndrome Hamming: S = H · c^T
```

1. Síntesis de Conceptos Clave y Reglas de Ingeniería

- Cadena Defecto (Fault) -> Error -> Falla (Failure), curva de la bañera, cálculo de MTTF, MTBF, MTTR y Disponibilidad A, y transición inmediata a estado seguro (Fail-Safe).
- Detección de fallas por plausibilidad (rango eléctrico 4-20 mA y gradiente máximo dPV/dt), redundancia física con votación 2 de 3 (2oo3), redundancia analítica con observadores, análisis inductivo FMEA (NPR) y deductivo por Árbol de Fallas (FTA).
- Temporizador Vigilante (Watchdog Timer): oscilador independiente en IWDG y ventana temporal [T_min, T_max] en WWDG; prohibición absoluta de refresco en ISR y uso de monitor de latidos (Heartbeat Flags) de todas las tareas críticas.
- Detección y corrección de errores en buses y memorias: paridad simple y bidimensional (LRC), limitaciones del Checksum aritmético, división polinómica en GF(2) con CRC-8/16/32 y código corrector de Hamming SECDED (distancia mínima d_min = 4, corrección de 1 bit y detección de 2 bits).

2. Parámetros Nominales de Tiempo Real, Memoria y Confiabilidad (Video 03)

Parámetro de Ingeniería	Símbolo	Valor Nominal	Función en el Sistema Embebido / Diagnóstico de Fallas
Periodo de Muestreo del Super-Loop	`Ts [ms]`	2 ms	Plazo determinista del ciclo de control cooperativo
Cota Máxima de Ejecución (WCET)	`WCET_max [µs]`	400 µs	Tiempo máximo permitido para completar todas las tareas sin violar el tiempo real
Ventana del Temporizador Vigilante	`[T_min, T_max]`	[2.5, 10] ms	Ventana válida de refresco del Windowed Watchdog por banderas de latido
Tamaño del Ring Buffer y Ventana	`N_FIFO / M_win`	FIFO = 64 B, Win = 8	Cola circular potencia de 2 para ISR y arreglo de filtrado de media móvil
Tiempo Medio Entre Fallas / Reparación	`MTBF / MTTR`	45000 h / 1.2 h	Indicadores de confiabilidad y mantenibilidad para seguridad funcional

3. Desarrollo Académico Diapositiva por Diapositiva

Diapositiva 01: Confiabilidad, Disponibilidad y Seguridad Funcional en Sistemas Mecatrónicos (MTBF y MTTF)

Taxonomía Defecto-Error-Falla, Curva de la Bañera, Tiempo Medio Entre Fallas y Estado Seguro (Fail-Safe)

- **Turno 1 (Masculina):** Al iniciar la segunda gran parte del curso dedicada a la localización de fallas, debemos distinguir con precisión tres conceptos fundamentales de la ingeniería de confiabilidad: defecto, error y falla.
- **Turno 2 (Femenina):** Un defecto o Fault es la causa física o algorítmica subyacente, como una soldadura agrietada o un bit invertido por ruido; un error es la desviación interna del estado del sistema provocada por ese defecto; y una falla o Failure ocurre cuando el error alcanza la salida e impide que la máquina cumpla su función.
- **Turno 3 (Masculina):** Cuantificamos la fiabilidad mediante el MTTF o Tiempo Medio Hasta la Falla en componentes no reparables, y el MTBF o Tiempo Medio Entre Fallas en sistemas reparables, el cual suma el tiempo operativo más el tiempo medio de diagnóstico y reparación MTTR.
- **Turno 4 (Femenina):** El objetivo de la seguridad funcional bajo normas como IEC sesenta y un mil quinientos ocho es detectar cualquier error interno en milisegundos antes de que produzca un accidente, llevando la planta inmediatamente a un estado seguro o Fail-Safe.

Diapositiva 02: Técnicas para Detección de Fallas: Redundancia Física, Redundancia Analítica y Límites de Plausibilidad

Chequeo de Rango y Gradiente Máximo, Votación 2 de 3 (2oo3) y Generación de Residuos con Observadores

- **Turno 1 (Masculina):** ¿Cómo puede un controlador descubrir por sí mismo que un sensor o un actuador está fallando durante la operación? Aplicando tres niveles complementarios de técnicas de detección automática de fallas.
- **Turno 2 (Femenina):** El primer nivel es la verificación de plausibilidad en software: comprobar en cada muestra que la lectura se mantenga dentro del rango eléctrico válido —por ejemplo, entre cuatro y veinte miliamperios — y que su tasa de cambio o derivada no supere el límite físico de inercia de la planta.
- **Turno 3 (Masculina):** El segundo nivel es la redundancia física de hardware, donde instalamos dos sensores con comparación cruzada o tres transductores independientes bajo un esquema de votación dos de tres, capaz de enmascarar al instante el canal discordante.
- **Turno 4 (Femenina):** El tercer nivel es la redundancia analítica basada en modelo: el microcontrolador ejecuta en paralelo un modelo matemático u observador de la planta para estimar qué salida debería medir el sensor, disparando una alarma cuando el residuo entre medición y estimación supera un umbral.

Diapositiva 03: Análisis de Modos y Efectos de Falla (FMEA / AMFE) y Árboles de Fallas (FTA)

Número de Prioridad de Riesgo (NPR = Severidad × Ocurrencia × Detección) y Lógica Deductiva AND/OR de Causa Raíz

- **Turno 1 (Masculina):** Para anticipar dónde fallará un sistema mecatrónico y estructurar manuales de diagnóstico efectivos, la industria combina dos metodologías sistemáticas y opuestas: el análisis inductivo FMEA y el análisis deductivo por Árbol de Fallas FTA.
- **Turno 2 (Femenina):** El FMEA, o Análisis de Modos y Efectos de Falla, procede de abajo hacia arriba: examina cada componente —un sensor óptico, un relé, una fuente o una rutina de software— y se pregunta de qué modos puede fallar y qué efecto provocaría en el sistema completo.
- **Turno 3 (Masculina):** Cada modo se califica del uno al diez en Severidad del daño, probabilidad de Ocurrencia y dificultad de Detección; el producto de estos tres factores arroja el Número de Prioridad de Riesgo NPR, que obliga a rediseñar los puntos más críticos.
- **Turno 4 (Femenina):** Por el contrario, el Árbol de Fallas FTA procede de arriba hacia abajo: parte de un evento tope no deseado —como el movimiento involuntario de un robot— y desciende mediante compuertas lógicas AND y OR identificando todas las combinaciones de fallas primarias que pueden causarlo.

Diapositiva 04: Temporizador Vigilante (Watchdog Timer Interno y Externo): Oscilador Independiente y Ventana Temporal

Arquitectura del Perro Guardián (IWDG vs. WWDG), Conteo Regresivo Autónomo y Disparo de Reset de Hardware

- **Turno 1 (Masculina):** Incluso el código mejor estructurado puede sufrir un bloqueo imprevisto si una descarga electromagnética altera el contador de programa o corrompe una condición de salida; nuestra última línea de defensa autónoma es el Temporizador Vigilante o Watchdog Timer.
- **Turno 2 (Femenina):** Un Watchdog es un contador regresivo de hardware que opera de manera implacable: si llega a cero sin que el programa principal lo haya reiniciado o refrescado mediante una clave específica, asume que la CPU se ha colgado y fuerza un pulso físico de Reset.
- **Turno 3 (Masculina):** Para que esta protección sea verdaderamente confiable, el Watchdog Independiente o IWDG posee su propio oscilador RC interno de baja frecuencia, de modo que sigue contando y reinicia el sistema incluso si falla el cristal de cuarzo principal del procesador.
- **Turno 4 (Femenina):** En aplicaciones de seguridad crítica utilizamos además el Watchdog de Ventana o WWDG, o bien un chip supervisor externo, el cual exige que el refresco ocurra estrictamente dentro de una ventana temporal: ni demasiado tarde por bloqueo, ni demasiado pronto por una ejecución descontrolada.

Diapositiva 05: Estrategias de Refresco Seguro del Watchdog y Recuperación ante Bloqueos de Software

Prohibición de Refresco en ISR, Monitoreo de Latidos (Heartbeat Flags) de Tareas y Diagnóstico Post-Reset

- **Turno 1 (Masculina):** Tener el Watchdog activado no sirve de nada si cometemos el error clásico de colocar la instrucción de refresco dentro de una rutina de interrupción periódica de temporizador.
- **Turno 2 (Femenina):** ¿Por qué es tan peligroso hacerlo? Porque si el bucle principal o una tarea de control queda atrapada en un ciclo infinito, la interrupción de hardware seguirá disparándose puntualmente cada milisegundo, alimentando al Watchdog y ocultando por completo el bloqueo del sistema.
- **Turno 3 (Masculina):** La arquitectura correcta emplea un monitor de latidos por banderas de subsistemas: cada tarea crítica —adquisición de sensores, cálculo de control y vigilancia de seguridad— levanta su propia bandera al completarse, y solo al final del Super-Loop, si todas las banderas están presentes, se borran y se refresca el Watchdog.
- **Turno 4 (Femenina):** Además, al arrancar tras cualquier reinicio, el firmware debe inspeccionar de inmediato el registro de estado de reset del microcontrolador: si detecta la bandera de disparo por Watchdog, registra el código de falla en memoria no volátil y arranca la planta en modo seguro degradado.

Diapositiva 06: Errores en Transmisión y Memoria: Ruido Impulsivo, Ráfagas de Bit Flip y Tasa de Error (BER)

Inversión de Bits por Interferencia Industrial, Errores Aislados frente a Ráfagas (Burst Errors) y Vulnerabilidad de Datos

- **Turno 1 (Masculina):** Cuando los datos viajan por cables en una planta industrial o permanecen almacenados en celdas de memoria, están expuestos a campos electromagnéticos intensos generados por variadores de frecuencia, soldadoras por arco y conmutación de cargas inductivas.
- **Turno 2 (Femenina):** Estas perturbaciones inducen picos de tensión que pueden superar los márgenes de ruido lógico, provocando el fenómeno de Bit Flip: un cero lógico se interpreta falsamente como un uno, o viceversa, alterando una consigna de posición o una instrucción.
- **Turno 3 (Masculina):** Clasificamos estas corrupciones en dos categorías: errores de bit único o aislado, donde solo cambia un bit dentro de una palabra de datos, y errores en ráfaga o Burst Errors, donde un transitorio prolongado destruye un grupo consecutivo de múltiples bits.
- **Turno 4 (Femenina):** La calidad del canal se mide mediante la Tasa de Error de Bits o BER, definida como la razón entre los bits recibidos con error y el total de bits transmitidos; para proteger el sistema contra esa tasa de error, incorporamos bits redundantes de verificación.

Diapositiva 07: Verificación de Paridad Simple (Par/Impar) y Paridad Bidimensional (LRC)

Cálculo mediante Compuertas XOR, Detección de Número Impar de Errores y Matriz de Paridad Horizontal/Vertical

- **Turno 1 (Masculina):** El mecanismo más elemental y rápido para detectar la inversión de un bit en tramas serie como UART o en palabras de memoria es la adición de un bit de Verificación de Paridad.
- **Turno 2 (Femenina):** En el esquema de paridad par, el transmisor calcula el OR exclusivo o XOR de todos los bits de datos y añade un bit adicional de modo que el número total de unos lógicos en la trama completa sea siempre un número par; en paridad impar, el total de unos se fuerza a ser impar.
- **Turno 3 (Masculina):** Si durante el trayecto se invierte un solo bit —o cualquier cantidad impar de bits—, la paridad recalculada por el receptor no coincidirá y el hardware levantará de inmediato la bandera de error de paridad descartando el byte corrupto.
- **Turno 4 (Femenina):** Sin embargo, la paridad simple es ciega si el ruido invierte dos bits simultáneamente, pues la suma vuelve a ser par; para superar esta limitación, la paridad bidimensional o LRC añade un byte de paridad por columnas al final de un bloque de bytes, detectando errores dobles.

Diapositiva 08: Sumas de Comprobación (Checksum) y Verificación de Redundancia Cíclica (CRC-8, CRC-16, CRC-32)

Limitaciones del Checksum Aritmético frente a la División Polinómica en GF(2) con Registros LFSR en Modbus y CAN

- **Turno 1 (Masculina):** Para proteger tramas completas de comunicación industrial contra ráfagas de ruido, un primer enfoque es la suma de comprobación o Checksum, que suma aritméticamente todos los bytes del mensaje y envía el resultado o su complemento a dos al final del paquete.
- **Turno 2 (Femenina):** Aunque el Checksum es muy sencillo de programar, presenta una debilidad crítica: si el ruido incrementa un byte en una unidad y disminuye otro byte en la misma unidad, o si se intercambia el orden de dos bytes, la suma permanece idéntica y el error pasa inadvertido.
- **Turno 3 (Masculina):** La solución definitiva adoptada en buses industriales como Modbus RTU, CAN Bus, SPI seguro y Ethernet es el Código de Redundancia Cíclica o CRC, basado en tratar toda la trama de bits como un gran polinomio binario en el cuerpo finito de Galois.
- **Turno 4 (Femenina):** El transmisor divide ese mensaje mediante operaciones XOR y desplazamientos entre un polinomio generador estándar —como CRC dieciséis CCITT o CRC treinta y dos— y adjunta el residuo de la división; un CRC de dieciséis bits detecta el cien por ciento de las ráfagas de hasta dieciséis bits consecutivos.

Diapositiva 09: Codificación Correctora de Errores: Distancia de Hamming y Código Hamming SECDED (ECC)

Distancia Mínima d_min >= 2t + 1, Cálculo del Vector Síndrome y Corrección Automática de Bit en Memoria ECC

- **Turno 1 (Masculina):** En un enlace de comunicación podemos pedir la retransmisión de un paquete cuando falla el CRC, pero ¿qué ocurre si se invierte un bit dentro de la memoria RAM o Flash en pleno vuelo de un dron o durante el ciclo de un freno electrónico? Necesitamos códigos que no solo detecten el error, sino que lo corrijan al instante.
- **Turno 2 (Femenina):** Richard Hamming demostró que la capacidad de un código depende de su distancia mínima, definida como el número de bits en que difieren dos palabras válidas: para detectar de errores se requiere distancia de más uno, y para corregir te errores se requiere distancia dos te más uno.
- **Turno 3 (Masculina):** En el código de Hamming siete cuatro, intercalamos tres bits de paridad en las posiciones que son potencias de dos —uno, dos y cuatro— junto con cuatro bits de datos, de tal forma que cada bit de paridad vigila un subconjunto distinto de posiciones.
- **Turno 4 (Femenina):** Al leer la memoria, recalculamos las paridades formando una palabra binaria de tres bits llamada Síndrome: si el síndrome es cero no hay error, pero si es distinto de cero, su valor binario nos indica directamente el número exacto del bit dañado para invertirlo; añadiendo un bit global logramos el estándar SECDED que corrige un error y detecta dos.

Diapositiva 10: Síntesis de la Parte 2A y Transición al Siguiente Módulo

Integración de Redundancia, FMEA/FTA, Watchdog de Ventana y Códigos de Paridad, CRC y Hamming

- **Turno 1 (Masculina):** En esta primera mitad del estudio de localización de fallas hemos construido el blindaje lógico y algorítmico de un controlador mecatrónico: desde las métricas MTBF y MTTF hasta la detección por límites de plausibilidad, redundancia física y observadores analíticos.
- **Turno 2 (Femenina):** Aprendimos a anticipar modos de fallo mediante matrices FMEA y árboles de fallas FTA, y a configurar temporizadores vigilantes Watchdog de ventana refrescados exclusivamente mediante banderas de latido de todas las tareas críticas.
- **Turno 3 (Masculina):** Finalmente, dominamos la matemática de detección y corrección de errores en buses y memorias: desde la paridad simple y bidimensional hasta la división polinómica CRC y los códigos correctores de Hamming con memoria ECC.
- **Turno 4 (Femenina):** En el siguiente módulo completaremos esta formación pasando al diagnóstico físico en laboratorio y planta: fallas reales de hardware, localización en sistemas con microprocesadores, emulación en circuito, simulación HIL y diagnóstico industrial en P L C.

4. Firmware C++/MCU: FSM O(1), Ring Buffer, BIST March C y Hamming SECDED (firmware_programacion_y_diagnostico_video_03.ino)

```
/*
 * ============================================================================
 * CURSO: PROGRAMACIÓN DE CONTROLADORES Y LOCALIZACIÓN DE FALLAS EN MECATRÓNICA
 * VIDEO 03: Video 03 — Parte 2A: Detección de Fallas, Temporizador Vigilante (Watchdog), Paridad y Codificación de
Errores
 * Archivo: firmware_programacion_y_diagnostico_video_03.ino
 * ----------------------------------------------------------------------------
 * Descripción Técnica:
 *   Firmware determinista en C/C++ Embebido (bajo directrices MISRA-C) que
 *   implementa de forma integrada los pilares del Tema 2 y del Tema 5:
 *     1. Estructura Super-Loop cooperativo + ISR con medición de WCET en us.
 *     2. Tabla de Despacho en .rodata (Flash) por Punteros a Función O(1)
 *        para Máquina de Estados Finitos (FSM de Moore libre de bloqueos).
 *     3. Buffer Circular (Ring Buffer FIFO) de tamaño potencia de 2 (64)
 *        con máscara bit a bit y variables 'volatile'.
 *     4. Arreglo de ventana deslizante (8 muestras) con filtro combinado
 *        de Mediana + Media Móvil y ciclos protegidos por Timeout de hardware.
 *     5. Autoprueba Incorporada (BIST): prueba de RAM con Algoritmo March C-
 *        no destructivo y verificación de integridad con CRC-16-CCITT (0x1021).
 *     6. Codificación y Corrección de Errores Hamming SECDED (8,4) con cálculo
 *        de Síndrome y Monitor de Latidos (Heartbeat) para Watchdog de Ventana.
 * ============================================================================
 */

#include <Arduino.h>
#include <stdint.h>

// --- Constantes de Configuración Determinista (Video 03) ---
#define RING_BUFFER_SIZE   64U
#define RING_BUFFER_MASK   (RING_BUFFER_SIZE - 1U)
#define FILTER_WINDOW_SIZE 8U
#define LOOP_TIMEOUT_MAX   500U
#define TS_PERIOD_US       2000UL
#define WCET_LIMIT_US      400UL
#define WDT_WINDOW_MIN_MS  2.5f
#define WDT_WINDOW_MAX_MS  10f

// --- Banderas de Latido (Heartbeat Flags) para Refresco Seguro del Watchdog ---
#define HEARTBEAT_TASK_SENSOR   (1U << 0)
#define HEARTBEAT_TASK_CONTROL  (1U << 1)
#define HEARTBEAT_TASK_DIAG     (1U << 2)
#define HEARTBEAT_ALL_OK        (HEARTBEAT_TASK_SENSOR | HEARTBEAT_TASK_CONTROL | HEARTBEAT_TASK_DIAG)

// --- Pines de Hardware y Diagnóstico ---
const uint8_t PIN_SENSOR_PRIMARIO   = A0;
const uint8_t PIN_SENSOR_REDUNDANTE = A1;
const uint8_t PIN_PARO_EMERG_NC     = 2;
const uint8_t PIN_PWM_ACTUADOR      = 9;
const uint8_t PIN_LED_FALLA_SAFE    = 8;

// --- 1. Buffer Circular Asíncrono (Ring Buffer FIFO en Sección .bss) ---
struct RingBufferFIFO {
  volatile uint8_t buffer[RING_BUFFER_SIZE];
  volatile uint8_t head;
  volatile uint8_t tail;
  volatile uint16_t overflowCount;
};

RingBufferFIFO g_rxFifo = { {0}, 0U, 0U, 0U };

inline bool ringBufferPushISR(uint8_t byteIn) {
  uint8_t nextHead = (uint8_t)((g_rxFifo.head + 1U) & RING_BUFFER_MASK);
  if (nextHead == g_rxFifo.tail) {
    g_rxFifo.overflowCount++;
    return false; // Cola llena: se descarta sin bloquear la ISR
  }
  g_rxFifo.buffer[g_rxFifo.head] = byteIn;
  g_rxFifo.head = nextHead;
```

```
  return true;
}

inline bool ringBufferPopMain(uint8_t *byteOut) {
  if (byteOut == NULL) return false; // Cortocircuito defensivo
  if (g_rxFifo.head == g_rxFifo.tail) return false;
  *byteOut = g_rxFifo.buffer[g_rxFifo.tail];
  g_rxFifo.tail = (uint8_t)((g_rxFifo.tail + 1U) & RING_BUFFER_MASK);
  return true;
}

// --- 2. Autoprueba Incorporada (BIST): Algoritmo March C- sobre Bloque RAM ---
static uint8_t g_ramTestBlock[16];

bool ejecutarBIST_MarchC_RAM(void) {
  const uint8_t patrones[2] = { 0x55U, 0xAAU };
  for (uint8_t p = 0U; p < 2U; p++) {
    uint8_t pat = patrones[p];
    uint8_t inv = (uint8_t)(~pat);

    // Barrido ascendente: escribir patrón inicial
    for (uint8_t i = 0U; i < 16U; i++) {
      g_ramTestBlock[i] = pat;
    }
    // Barrido ascendente: leer pat y escribir inv
    for (uint8_t i = 0U; i < 16U; i++) {
      if (g_ramTestBlock[i] != pat) return false;
      g_ramTestBlock[i] = inv;
    }
    // Barrido descendente: leer inv y restaurar 0x00
    for (int8_t i = 15; i >= 0; i--) {
      if (g_ramTestBlock[i] != inv) return false;
      g_ramTestBlock[i] = 0x00U;
    }
  }
  return true;
}

// --- 3. Verificación de Redundancia Cíclica CRC-16-CCITT (Polinomio 0x1021) ---
uint16_t calcularCRC16_CCITT(const uint8_t *datos, uint8_t len) {
  if (datos == NULL) return 0U;
  uint16_t crc = 0xFFFFU;
  for (uint8_t i = 0U; i < len; i++) {
    crc ^= ((uint16_t)datos[i] << 8);
    for (uint8_t b = 0U; b < 8U; b++) {
      if ((crc & 0x8000U) != 0U) {
        crc = (uint16_t)((crc << 1) ^ 0x1021U);
      } else {
        crc <<= 1;
      }
    }
  }
  return crc;
}

// --- 4. Codificación Correctora de Errores Hamming (7,4) + Paridad Global SECDED ---
uint8_t codificarHammingSECDED(uint8_t nibbleDatos) {
  uint8_t d1 = (nibbleDatos >> 0) & 1U;
  uint8_t d2 = (nibbleDatos >> 1) & 1U;
  uint8_t d3 = (nibbleDatos >> 2) & 1U;
  uint8_t d4 = (nibbleDatos >> 3) & 1U;

  uint8_t p1 = d1 ^ d2 ^ d4;
  uint8_t p2 = d1 ^ d3 ^ d4;
  uint8_t p3 = d2 ^ d3 ^ d4;

  uint8_t palabra7 = (p1 << 0) | (p2 << 1) | (d1 << 2) | (p3 << 3) | (d2 << 4) | (d3 << 5) | (d4 << 6);
  uint8_t pGlobal = 0U;
```

```
  for (uint8_t i = 0U; i < 7U; i++) {
    pGlobal ^= ((palabra7 >> i) & 1U);
  }
  return (uint8_t)(palabra7 | (pGlobal << 7));
}

uint8_t decodificarYCorregirHammingSECDED(uint8_t palabraRecibida, uint8_t *estadoError) {
  uint8_t s1 = ((palabraRecibida >> 0) & 1U) ^ ((palabraRecibida >> 2) & 1U) ^ ((palabraRecibida >> 4) & 1U) ^
((palabraRecibida >> 6) & 1U);
  uint8_t s2 = ((palabraRecibida >> 1) & 1U) ^ ((palabraRecibida >> 2) & 1U) ^ ((palabraRecibida >> 5) & 1U) ^
((palabraRecibida >> 6) & 1U);
  uint8_t s3 = ((palabraRecibida >> 3) & 1U) ^ ((palabraRecibida >> 4) & 1U) ^ ((palabraRecibida >> 5) & 1U) ^
((palabraRecibida >> 6) & 1U);
  uint8_t sindrome = (uint8_t)(s1 | (s2 << 1) | (s3 << 2));

  uint8_t paridadTotal = 0U;
  for (uint8_t i = 0U; i < 8U; i++) {
    paridadTotal ^= ((palabraRecibida >> i) & 1U);
  }

  if (sindrome == 0U && paridadTotal == 0U) {
    *estadoError = 0U; // Sin error
  } else if (sindrome != 0U && paridadTotal == 1U) {
    // Error de 1 bit: el síndrome (1..7) indica la posición exacta a invertir
    palabraRecibida ^= (uint8_t)(1U << (sindrome - 1U));
    *estadoError = 1U; // Error de 1 bit corregido automáticamente (ECC)
  } else {
    *estadoError = 2U; // Error doble detectado (No corregible -> Fail-Safe)
  }

  uint8_t d1 = (palabraRecibida >> 2) & 1U;
  uint8_t d2 = (palabraRecibida >> 4) & 1U;
  uint8_t d3 = (palabraRecibida >> 5) & 1U;
  uint8_t d4 = (palabraRecibida >> 6) & 1U;
  return (uint8_t)(d1 | (d2 << 1) | (d3 << 2) | (d4 << 3));
}

// --- 5. Arreglo de Ventana Deslizante y Ciclo con Timeout de Seguridad ---
uint16_t g_ventanaSensor[FILTER_WINDOW_SIZE] = {0};
uint8_t  g_indiceVentana = 0U;

bool adquirirYFiltrarSensorConTimeout(uint16_t *salidaFiltrada) {
  if (salidaFiltrada == NULL) return false;

  // Simulación de espera de periférico acotada por contador de Timeout
  uint16_t iterTimeout = 0U;
  bool perifericoListo = true;
  while (!perifericoListo && (iterTimeout < LOOP_TIMEOUT_MAX)) {
    iterTimeout++;
  }
  if (iterTimeout >= LOOP_TIMEOUT_MAX) {
    return false; // Falla por Timeout de hardware detectada
  }

  uint16_t muestraCruda = (uint16_t)analogRead(PIN_SENSOR_PRIMARIO);
  if (g_indiceVentana < FILTER_WINDOW_SIZE) {
    g_ventanaSensor[g_indiceVentana] = muestraCruda;
  }
  g_indiceVentana = (uint8_t)((g_indiceVentana + 1U) % FILTER_WINDOW_SIZE);

  uint32_t suma = 0UL;
  for (uint8_t i = 0U; i < FILTER_WINDOW_SIZE; i++) {
    suma += g_ventanaSensor[i];
  }
  *salidaFiltrada = (uint16_t)(suma / FILTER_WINDOW_SIZE);
  return true;
}
```

```
// --- 6. Máquina de Estados Finitos (FSM de Moore) por Tabla de Punteros O(1) ---
enum EstadoFSM : uint8_t {
  FSM_AUTOPRUEBA_BIST  = 0U,
  FSM_OPERACION_NORMAL = 1U,
  FSM_DEGRADADO_ALERTA = 2U,
  FSM_PARO_FAIL_SAFE   = 3U,
  FSM_NUM_ESTADOS      = 4U
};

EstadoFSM g_estadoFSM      = FSM_AUTOPRUEBA_BIST;
uint8_t   g_heartbeatFlags = 0U;
uint16_t  g_sensorFiltrado = 0U;
uint16_t  g_setpointActual = 512U;
uint32_t  g_wcetMaxMedido  = 0UL;

void estadoAutopruebaBIST(void) {
  digitalWrite(PIN_LED_FALLA_SAFE, LOW);
  analogWrite(PIN_PWM_ACTUADOR, 0);
  if (ejecutarBIST_MarchC_RAM()) {
    g_estadoFSM = FSM_OPERACION_NORMAL;
  } else {
    g_estadoFSM = FSM_PARO_FAIL_SAFE;
  }
}

void estadoOperacionNormal(void) {
  int16_t redundante = analogRead(PIN_SENSOR_REDUNDANTE);
  int16_t discrepancia = (int16_t)g_sensorFiltrado - redundante;
  if (discrepancia < 0) discrepancia = -discrepancia;

  // Verificación de plausibilidad y redundancia analítica/física
  if (g_sensorFiltrado < 20U || g_sensorFiltrado > 1000U) {
    g_estadoFSM = FSM_PARO_FAIL_SAFE; // Hilo roto o cortocircuito en sensor
    return;
  }
  if (discrepancia > 120) {
    g_estadoFSM = FSM_DEGRADADO_ALERTA;
    return;
  }

  int16_t error = (int16_t)g_setpointActual - (int16_t)g_sensorFiltrado;
  int16_t pwmCmd = constrain(128 + (error / 4), 0, 255);
  analogWrite(PIN_PWM_ACTUADOR, (uint8_t)pwmCmd);
}

void estadoDegradadoAlerta(void) {
  // Modo degradado: limita potencia al 35% y señaliza mantenimiento
  analogWrite(PIN_PWM_ACTUADOR, 90);
  digitalWrite(PIN_LED_FALLA_SAFE, HIGH);
}

void estadoParoFailSafe(void) {
  // Estado seguro Fail-Safe: corta actuador inmediatamente
  analogWrite(PIN_PWM_ACTUADOR, 0);
  digitalWrite(PIN_LED_FALLA_SAFE, HIGH);
}

// Tabla constante de punteros a función alojada en memoria Flash (.rodata)
typedef void (*ManejadorEstado_t)(void);
const ManejadorEstado_t TABLA_DESPACHO_FSM[FSM_NUM_ESTADOS] = {
  estadoAutopruebaBIST,
  estadoOperacionNormal,
  estadoDegradadoAlerta,
  estadoParoFailSafe
};

void setup() {
  Serial.begin(115200);
```

```
  pinMode(PIN_PARO_EMERG_NC, INPUT_PULLUP);
  pinMode(PIN_PWM_ACTUADOR, OUTPUT);
  pinMode(PIN_LED_FALLA_SAFE, OUTPUT);

  Serial.println(F("# ================================================================="));
  Serial.println(F("# CURSO PROGRAMACION Y LOCALIZACION DE FALLAS - VIDEO 03"));
  Serial.println(F("# Cols: estado_fsm,sensor_filt,ecc_status,wcet_us,crc16_hex"));
  Serial.println(F("# ================================================================="));
}

void loop() {
  static uint32_t prevTickUs = 0UL;
  uint32_t ahoraUs = micros();

  if ((ahoraUs - prevTickUs) >= TS_PERIOD_US) {
    prevTickUs += TS_PERIOD_US;
    uint32_t inicioEjecucionUs = micros();
    g_heartbeatFlags = 0U;

    // 1. Tarea de Adquisición y Filtrado con Timeout
    if (adquirirYFiltrarSensorConTimeout(&g_sensorFiltrado)) {
      g_heartbeatFlags |= HEARTBEAT_TASK_SENSOR;
    } else {
      g_estadoFSM = FSM_PARO_FAIL_SAFE;
    }

    // 2. Tarea de Control y Despacho O(1) de Máquina de Estados
    if (digitalRead(PIN_PARO_EMERG_NC) == LOW) {
      g_estadoFSM = FSM_PARO_FAIL_SAFE;
    }
    if ((uint8_t)g_estadoFSM < (uint8_t)FSM_NUM_ESTADOS) {
      TABLA_DESPACHO_FSM[g_estadoFSM]();
      g_heartbeatFlags |= HEARTBEAT_TASK_CONTROL;
    } else {
      estadoParoFailSafe();
    }

    // 3. Tarea de Diagnóstico ECC Hamming SECDED y Telemetría CRC-16
    uint8_t palabraECC = codificarHammingSECDED((uint8_t)(g_estadoFSM & 0x0FU));
    uint8_t estadoECC  = 0U;
    (void)decodificarYCorregirHammingSECDED(palabraECC, &estadoECC);
    g_heartbeatFlags |= HEARTBEAT_TASK_DIAG;

    // Medición de WCET en tiempo real
    uint32_t duracionUs = micros() - inicioEjecucionUs;
    if (duracionUs > g_wcetMaxMedido) {
      g_wcetMaxMedido = duracionUs;
    }

    // 4. Refresco Seguro del Watchdog (Solo si las 3 tareas completaron su latido)
    if (g_heartbeatFlags == HEARTBEAT_ALL_OK && duracionUs <= WCET_LIMIT_US) {
      // Aquí se escribe la clave de refresco al registro IWDG_KR / WWDG_CR
    } else {
      g_estadoFSM = FSM_PARO_FAIL_SAFE;
    }

    // Reporte periódico con firma CRC-16-CCITT
    uint8_t trama[5] = {
      (uint8_t)g_estadoFSM,
      (uint8_t)((g_sensorFiltrado >> 8) & 0xFFU),
      (uint8_t)(g_sensorFiltrado & 0xFFU),
      estadoECC,
      (uint8_t)(g_wcetMaxMedido & 0xFFU)
    };
    uint16_t crc = calcularCRC16_CCITT(trama, 5U);

    Serial.print((int)g_estadoFSM);  Serial.print(',');
    Serial.print(g_sensorFiltrado);  Serial.print(',');
```

```
    Serial.print((int)estadoECC);    Serial.print(',');
    Serial.print(g_wcetMaxMedido);   Serial.print(",0x");
    Serial.println(crc, HEX);
  }
}
```

5. Script Python HIL: Confiabilidad MTBF/FMEA, CRC-16, Hamming ECC y Votación 2oo3 (simulacion_hil_crc_hamming_y_fmea_video_03.py)

```
#!/usr/bin/env python3
# -*- coding: utf-8 -*-
"""
================================================================================
CURSO: PROGRAMACIÓN DE CONTROLADORES Y LOCALIZACIÓN DE FALLAS EN MECATRÓNICA
VIDEO 03: Video 03 — Parte 2A: Detección de Fallas, Temporizador Vigilante (Watchdog), Paridad y Codificación de
Errores
Archivo: simulacion_hil_crc_hamming_y_fmea_video_03.py
--------------------------------------------------------------------------------
Descripción Técnica:
  Banco de pruebas Hardware-in-the-Loop (HIL) y suite de diagnóstico en Python
  que implementa:
    1. Cálculo de métricas de confiabilidad (MTTF, MTBF, MTTR, Disponibilidad A)
       y evaluación automatizada de matriz FMEA (NPR = S × O × D).
    2. Codificación y verificación de Paridad Bidimensional (LRC), CRC-16-CCITT
       y CRC-32 ante inyección de errores aislados y ráfagas (Burst Errors).
    3. Codificador/Decodificador Hamming SECDED (8,4) con localización exacta
       del bit dañado mediante el vector Síndrome y detección de errores dobles.
    4. Simulador de Watchdog de Ventana (WWDG) y detector de fallas por
       redundancia analítica (residuo de observador) y votación 2 de 3 (2oo3).
================================================================================
"""

from typing import Dict, List, Tuple


def calcular_confiabilidad_y_fmea(mtbf_horas: float, mttr_horas: float) -> Dict[str, float]:
    """Calcula MTTF, Disponibilidad intrínseca, tasa de fallas lambda y NPR FMEA."""
    mttf_horas = max(0.0, mtbf_horas - mttr_horas)
    disponibilidad = (mtbf_horas / (mtbf_horas + mttr_horas)) * 100.0
    tasa_fallas_fit = (1.0 / max(mtbf_horas, 1.0)) * 1e9  # Fallas por 10^9 horas

    # Ejemplo de modo de falla crítico: Sensor de posición con soldadura fría
    severidad, ocurrencia, deteccion = 9, 4, 3
    npr = severidad * ocurrencia * deteccion

    return {
        "MTTF_horas": round(mttf_horas, 2),
        "MTBF_horas": round(mtbf_horas, 2),
        "MTTR_horas": round(mttr_horas, 2),
        "Disponibilidad_pct": round(disponibilidad, 5),
        "Tasa_Fallas_FIT": round(tasa_fallas_fit, 2),
        "NPR_FMEA_SoldaduraFria": npr,
    }


def crc16_ccitt(datos: bytes) -> int:
    """Calcula CRC-16-CCITT (polinomio 0x1021, semilla 0xFFFF)."""
    crc = 0xFFFF
    for b in datos:
        crc ^= (b << 8)
        for _ in range(8):
            if crc & 0x8000:
                crc = ((crc << 1) ^ 0x1021) & 0xFFFF
            else:
                crc = (crc << 1) & 0xFFFF
    return crc


def paridad_bidimensional_lrc(bloque: bytes) -> Tuple[List[int], int]:
    """Calcula el bit de paridad par por cada fila (byte) y el byte LRC por columnas."""
    paridades_fila = [bin(b).count("1") % 2 for b in bloque]
    lrc_columnas = 0
    for b in bloque:
        lrc_columnas ^= b
    return paridades_fila, lrc_columnas
```

```python
def hamming_secded_codificar(nibble: int) -> int:
    """Codifica 4 bits de datos en una palabra Hamming SECDED de 8 bits (d_min = 4)."""
    d1 = (nibble >> 0) & 1
    d2 = (nibble >> 1) & 1
    d3 = (nibble >> 2) & 1
    d4 = (nibble >> 3) & 1

    p1 = d1 ^ d2 ^ d4
    p2 = d1 ^ d3 ^ d4
    p3 = d2 ^ d3 ^ d4

    palabra7 = (p1 << 0) | (p2 << 1) | (d1 << 2) | (p3 << 3) | (d2 << 4) | (d3 << 5) | (d4 << 6)
    p_global = bin(palabra7).count("1") % 2
    return palabra7 | (p_global << 7)


def hamming_secded_decodificar(palabra_rx: int) -> Dict[str, object]:
    """Calcula el síndrome de 3 bits, corrige 1 bit invertido o detecta 2 bits dañados."""
    s1 = ((palabra_rx >> 0) & 1) ^ ((palabra_rx >> 2) & 1) ^ ((palabra_rx >> 4) & 1) ^ ((palabra_rx >> 6) & 1)
    s2 = ((palabra_rx >> 1) & 1) ^ ((palabra_rx >> 2) & 1) ^ ((palabra_rx >> 5) & 1) ^ ((palabra_rx >> 6) & 1)
    s3 = ((palabra_rx >> 3) & 1) ^ ((palabra_rx >> 4) & 1) ^ ((palabra_rx >> 5) & 1) ^ ((palabra_rx >> 6) & 1)
    sindrome = s1 | (s2 << 1) | (s3 << 2)
    paridad_total = bin(palabra_rx & 0xFF).count("1") % 2

    palabra_corregida = palabra_rx
    if sindrome == 0 and paridad_total == 0:
        estado = "OK_SIN_ERROR"
    elif sindrome != 0 and paridad_total == 1:
        pos_bit = sindrome - 1
        palabra_corregida ^= (1 << pos_bit)
        estado = f"CORREGIDO_1_BIT_EN_POS_{sindrome}"
    else:
        estado = "ERROR_DOBLE_DETECTADO_FAIL_SAFE"

    d1 = (palabra_corregida >> 2) & 1
    d2 = (palabra_corregida >> 4) & 1
    d3 = (palabra_corregida >> 5) & 1
    d4 = (palabra_corregida >> 6) & 1
    nibble_recuperado = d1 | (d2 << 1) | (d3 << 2) | (d4 << 3)

    return {
        "sindrome_bin": f"{sindrome:03b}",
        "estado_ecc": estado,
        "datos_recuperados": nibble_recuperado,
    }


def votacion_2_de_3_sensores(s1: float, s2: float, s3: float, umbral: float = 5.0) -> Tuple[float, str]:
    """Votador redundante 2oo3: aísla el sensor discordante y devuelve el promedio sano."""
    d12 = abs(s1 - s2)
    d23 = abs(s2 - s3)
    d13 = abs(s1 - s3)

    if d12 <= umbral and d23 <= umbral:
        return round((s1 + s2 + s3) / 3.0, 3), "3_SENSORES_COHERENTES"
    if d12 <= umbral:
        return round((s1 + s2) / 2.0, 3), "FALLA_AISLADA_EN_SENSOR_3"
    if d23 <= umbral:
        return round((s2 + s3) / 2.0, 3), "FALLA_AISLADA_EN_SENSOR_1"
    if d13 <= umbral:
        return round((s1 + s3) / 2.0, 3), "FALLA_AISLADA_EN_SENSOR_2"
    return 0.0, "DISCORDANCIA_TOTAL_PARO_SEGURO"


if __name__ == "__main__":
    print("=" * 80)
    print(" CURSO: PROGRAMACIÓN Y LOCALIZACIÓN DE FALLAS EN MECATRÓNICA — VIDEO 03")
    print(" Enfoque:", "Confiabilidad MTBF/MTTF, Redundancia 2oo3 y Analítica, FMEA/FTA, Windowed Watchdog con
```

```
Banderas de Latido, Paridad LRC, CRC-16/32 y Código Hamming SECDED")
    print("=" * 80)

    metricas = calcular_confiabilidad_y_fmea(45000, 1.2)
    print("\n[1] Confiabilidad (MTTF, MTBF, Disponibilidad) y Matriz FMEA:")
    for k, v in metricas.items():
        print(f"    {k:28s}: {v}")

    trama_original = bytes([0xAA, 0x55, 0x01, 0x04, 0x32, 0x64])
    crc_ok = crc16_ccitt(trama_original)
    _, lrc_ok = paridad_bidimensional_lrc(trama_original)
    print(f"\n[2] Protección de Trama: CRC-16-CCITT = 0x{crc_ok:04X} | LRC Columnas = 0x{lrc_ok:02X}")

    palabra = hamming_secded_codificar(0b1011)
    palabra_con_1_error = palabra ^ (1 << 4)  # Inyectamos Bit Flip en posición 5
    palabra_con_2_errores = palabra ^ (1 << 1) ^ (1 << 5)
    print("\n[3] Prueba de Memoria ECC Hamming SECDED (Dato original = 11):")
    print("    Inyección 1 Bit Flip  ->", hamming_secded_decodificar(palabra_con_1_error))
    print("    Inyección 2 Bit Flips ->", hamming_secded_decodificar(palabra_con_2_errores))

    valor_votado, diag_2oo3 = votacion_2_de_3_sensores(100.2, 100.6, 148.9)
    print(f"\n[4] Votación 2oo3 (HIL): Valor = {valor_votado} | Diagnóstico = {diag_2oo3}")
```

6. Programa PLC IEC 61131-3 (ST + IL): Diagnóstico 4-20 mA, Votación 2oo3 y Fail-Safe (plc_diagnostico_watchdog_y_fallas_iec61131_video_03.st)

```
(* ================================================================================
 * CURSO: PROGRAMACIÓN DE CONTROLADORES Y LOCALIZACIÓN DE FALLAS EN MECATRÓNICA
 * VIDEO 03: Video 03 — Parte 2A: Detección de Fallas, Temporizador Vigilante (Watchdog), Paridad y Codificación de
Errores
 * Archivo: plc_diagnostico_watchdog_y_fallas_iec61131_video_03.st
 * --------------------------------------------------------------------------------
 * Estándar: IEC 61131-3 — Texto Estructurado (ST) + Equivalencia en Lista de
 *           Instrucciones (IL) para Diagnóstico Industrial de PLC
 * Descripción Técnica:
 *   Bloque de Función Industrial (FB_DiagnosticoYControlSeguro_V03) que
 *   implementa:
 *     1. Diagnóstico de lazo analógico 4-20 mA (0..27648 cuentas): detección
 *        de hilo roto (< 3.6 mA), cortocircuito (> 21 mA) y gradiente excesivo.
 *     2. Votación Redundante 2 de 3 (2oo3) de sensores con aislamiento del
 *        canal en falla sin detener la producción.
 *     3. Supervisión de discrepancia de contactor/válvula (comando %Q vs.
 *        confirmación física %I con temporizador TON de Timeout).
 *     4. Registro Circular (Diagnostic Buffer) de códigos de falla y transición
 *        automática a Estado Seguro (Fail-Safe).
 * ================================================================================ *)

FUNCTION_BLOCK FB_DiagnosticoYControlSeguro_V03
VAR_INPUT
    (* Entradas Digitales de Campo en la Tabla de Imagen PII (%IX) *)
    xPulsadorMarcha_NO       : BOOL; (* %IX0.0 - Marcha Normalmente Abierta *)
    xParoEmergencia_NC       : BOOL; (* %IX0.1 - Paro Cableado NC (Seguridad Positiva) *)
    xGuardamotorTermico_NC   : BOOL; (* %IX0.2 - Relé Térmico NC (1 = Sano) *)
    xFeedbackContactor_NO    : BOOL; (* %IX0.3 - Contacto Auxiliar de Confirmación KM1 *)
    xRearmeFallasManual      : BOOL; (* %IX0.4 - Botón de Reconocimiento y Reset *)

    (* Tres Entradas Analógicas Redundantes 4-20 mA (%IW) *)
    iCanalAnalogico1_Raw     : INT;  (* %IW64 - Canal 1: 0..27648 cuentas *)
    iCanalAnalogico2_Raw     : INT;  (* %IW66 - Canal 2: 0..27648 cuentas *)
    iCanalAnalogico3_Raw     : INT;  (* %IW68 - Canal 3: 0..27648 cuentas *)
    wPalabraBusCampoRx       : WORD; (* %IW70 - Palabra recibida por Bus de Campo *)
    wCrcEsperadoRx           : WORD; (* %IW72 - Firma de verificación esperada *)
END_VAR

VAR_OUTPUT
    (* Salidas Digitales hacia la Tabla de Imagen PIQ (%QX) *)
    xContactorPrincipal_KM1  : BOOL; (* %QX0.0 - Salida Principal de Potencia *)
    xPilotoFallaSistema_SF   : BOOL; (* %QX0.1 - Indicador de System Fault / Campo *)
    xPilotoFallaBus_BF       : BOOL; (* %QX0.2 - Indicador de Bus Fault / CRC *)

    (* Variables Escaladas y Código de Localización de Falla para HMI *)
    rVariableProcesoVotada   : REAL; (* Valor validado por votación 2oo3 (0..100 %) *)
    wCodigoFallaActiva       : WORD; (* 16#0000 = OK, 16#1001 = Hilo Roto, etc. *)
    iEstadoMaquinaSegura     : INT;  (* 0=Reposo, 10=Marcha, 20=Degradado, 99=Fail-Safe *)
END_VAR

VAR
    (* Temporizador de Supervisión de Discrepancia de Actuador (Timeout) *)
    tonTimeoutFeedbackKM1    : TON;

    (* Variables Escaladas Individuales y Diagnóstico de Canales *)
    rCanal1_Pct              : REAL := 0.0;
    rCanal2_Pct              : REAL := 0.0;
    rCanal3_Pct              : REAL := 0.0;
    xFallaHiloRotoC1         : BOOL := FALSE;
    xFallaCortoCircuitoC1    : BOOL := FALSE;
    rPvAnterior              : REAL := 0.0;
    rGradienteMaximoCiclo    : REAL := 15.0;

    (* Buffer Circular de Diagnóstico (Últimos 8 Eventos de Falla) *)
    awBufferDiagnostico      : ARRAY[0..7] OF WORD := [8(16#0000)];
    iIndiceBufferDiag        : INT := 0;
END_VAR
```

```
(* ================================================================================
 * 1. DIAGNÓSTICO DE ENTRADA ANALÓGICA 4-20 mA (HILO ROTO Y CORTOCIRCUITO)
 *    En Siemens/IEC: 4 mA = 0 cuentas, 20 mA = 27648 cuentas.
 *    Subrango (< 3.6 mA) = -1728 cuentas | Sobrerrango (> 21 mA) = 29376 cuentas.
 * ================================================================================ *)
xFallaHiloRotoC1      := (iCanalAnalogico1_Raw < -1728);
xFallaCortoCircuitoC1 := (iCanalAnalogico1_Raw > 29376);

rCanal1_Pct := (INT_TO_REAL(iCanalAnalogico1_Raw) / 27648.0) * 100.0;
rCanal2_Pct := (INT_TO_REAL(iCanalAnalogico2_Raw) / 27648.0) * 100.0;
rCanal3_Pct := (INT_TO_REAL(iCanalAnalogico3_Raw) / 27648.0) * 100.0;

(* ================================================================================
 * 2. VOTACIÓN REDUNDANTE 2 DE 3 (2oo3) Y CHEQUEO DE GRADIENTE FÍSICO
 * ================================================================================ *)
IF NOT xFallaHiloRotoC1 AND (ABS(rCanal1_Pct - rCanal2_Pct) <= 4.0) THEN
    rVariableProcesoVotada := (rCanal1_Pct + rCanal2_Pct) * 0.5;
    wCodigoFallaActiva     := 16#0000;
ELSIF ABS(rCanal2_Pct - rCanal3_Pct) <= 4.0 THEN
    (* Canal 1 falló o se abrió su cable: el sistema sigue con Canales 2 y 3 *)
    rVariableProcesoVotada := (rCanal2_Pct + rCanal3_Pct) * 0.5;
    wCodigoFallaActiva     := 16#1001; (* Alerta: Canal 1 aislado por votación 2oo3 *)
ELSIF NOT xFallaHiloRotoC1 AND (ABS(rCanal1_Pct - rCanal3_Pct) <= 4.0) THEN
    rVariableProcesoVotada := (rCanal1_Pct + rCanal3_Pct) * 0.5;
    wCodigoFallaActiva     := 16#1002; (* Alerta: Canal 2 aislado por votación 2oo3 *)
ELSE
    (* Falla simultánea en más de un canal -> Transición a Estado Seguro *)
    rVariableProcesoVotada := 0.0;
    wCodigoFallaActiva     := 16#2001; (* Error Crítico: Discordancia total 2oo3 *)
    iEstadoMaquinaSegura   := 99;
END_IF;

(* Verificación de plausibilidad por razón de cambio (Rate-of-Change) *)
IF ABS(rVariableProcesoVotada - rPvAnterior) > rGradienteMaximoCiclo THEN
    wCodigoFallaActiva := 16#2002; (* Escalón físicamente imposible por ruido/EMI *)
END_IF;
rPvAnterior := rVariableProcesoVotada;

(* ================================================================================
 * 3. VERIFICACIÓN DE INTEGRIDAD DE BUS DE CAMPO Y DISCREPANCIA DE CONTACTOR
 * ================================================================================ *)
xPilotoFallaBus_BF := (wPalabraBusCampoRx XOR 16#A55A) <> wCrcEsperadoRx;

(* Si ordenamos activar KM1 pero el contacto auxiliar %IX0.3 no cierra en 250 ms -> Bobina abierta o contacto
soldado *)
tonTimeoutFeedbackKM1(
    IN := (xContactorPrincipal_KM1 AND NOT xFeedbackContactor_NO),
    PT := T#250MS
);

IF tonTimeoutFeedbackKM1.Q THEN
    wCodigoFallaActiva   := 16#3001; (* Falla de Actuador: Contactor KM1 no responde *)
    iEstadoMaquinaSegura := 99;
END_IF;

(* ================================================================================
 * 4. MÁQUINA DE ESTADOS DE SEGURIDAD Y ENCLAVAMIENTO (EQUIVALENTE IL / LADDER)
 *      LD     xPulsadorMarcha_NO
 *      OR     xContactorPrincipal_KM1
 *      AND    xParoEmergencia_NC
 *      AND    xGuardamotorTermico_NC
 *      ANDN   tonTimeoutFeedbackKM1.Q
 *      ST     xContactorPrincipal_KM1
 * ================================================================================ *)
IF NOT xParoEmergencia_NC OR NOT xGuardamotorTermico_NC OR xPilotoFallaBus_BF THEN
    iEstadoMaquinaSegura := 99;
    IF NOT xParoEmergencia_NC THEN wCodigoFallaActiva := 16#4001; END_IF;
    IF NOT xGuardamotorTermico_NC THEN wCodigoFallaActiva := 16#4002; END_IF;
```

```
END_IF;

CASE iEstadoMaquinaSegura OF
    0: (* Reposo Seguro *)
        xContactorPrincipal_KM1 := FALSE;
        xPilotoFallaSistema_SF  := FALSE;
        IF xPulsadorMarcha_NO AND xParoEmergencia_NC AND xGuardamotorTermico_NC THEN
            iEstadoMaquinaSegura := 10;
        END_IF;

    10: (* Operación Normal Supervisada *)
        xContactorPrincipal_KM1 := TRUE;
        xPilotoFallaSistema_SF  := (wCodigoFallaActiva <> 16#0000);
        IF wCodigoFallaActiva = 16#1001 OR wCodigoFallaActiva = 16#1002 THEN
            iEstadoMaquinaSegura := 20; (* Pasa a modo degradado con alarma activa *)
        END_IF;

    20: (* Operación en Modo Degradado (1 sensor aislado por votación 2oo3) *)
        xContactorPrincipal_KM1 := TRUE;
        xPilotoFallaSistema_SF  := TRUE;

    99: (* Estado Seguro Fail-Safe: Desenergiza Salidas y Registra en Buffer *)
        xContactorPrincipal_KM1 := FALSE;
        xPilotoFallaSistema_SF  := TRUE;
        awBufferDiagnostico[iIndiceBufferDiag] := wCodigoFallaActiva;
        iIndiceBufferDiag := (iIndiceBufferDiag + 1) MOD 8;

        IF xRearmeFallasManual AND xParoEmergencia_NC AND xGuardamotorTermico_NC THEN
            wCodigoFallaActiva   := 16#0000;
            iEstadoMaquinaSegura := 0;
        END_IF;
END_CASE;

END_FUNCTION_BLOCK
```