

Progetto di controllori logici

INGEGNERIA E TECNOLOGIE DEI SISTEMI DI CONTROLLO T

Tema n°2 - Lavatrice

1. Descrizione della logica di funzionamento nominale:

Il controllo logico della lavatrice implementato rispetta i dettagli e le specifiche di funzionamento menzionate nel testo descrittivo di consegna del progetto. Si specificano di seguito i comportamenti previsti rispetto alle scelte arbitrarie possibili:

- ✚ **INPUT PENDING**: Alla pressione del pulsante di Run (OFF→ON) non si ha l'avvio del comportamento nominale della lavatrice finché non sono verificate contemporaneamente le condizioni iniziali richieste, cioè la selezione di una temperatura e di un valore di programma coerenti con quelli predisposti, la chiusura dello sportello e la presenza del sapone se il programma selezionato lo richiede. In particolare, si salvano in variabili ausiliarie i valori di programma e temperatura selezionati tramite HMI, la verifica avviene così sulle variabili ausiliarie in modo da non potere modificare questi due input sino alla fase di check successiva. In particolare, si è scelto che alla pressione di Run (OFF→ON) si entra in una condizione di Pending, cioè di attesa di un corretto inserimento degli input tramite HMI, durante la quale vengono segnalate all'utente le anomalie relative alle verifiche suddette tramite apposite spie luminose. Se le variabili di interfaccia utente rispettano le condizioni previste si ha il blocco dello sportello e l'avvio della lavatrice secondo il programma selezionato. Come anticipato il programma e la temperatura scelti dall'utente sono salvati in variabili ausiliarie non modificabili se non nella fase di check successiva che a questo punto avverrà al termine del programma corrente.
- ✚ **WMCYCLE END**: Terminata l'esecuzione del programma impostato si ha una segnalazione visiva della conclusione di tutte le fasi tramite il lampeggio intermittente dei 3 Led di stato, cioè quelle spie luminose che durante l'esecuzione di un programma evidenziano il nome della fase che la lavatrice sta attuando in quel momento. Tale lampeggio suggerisce all'utente di premere nuovamente il pulsante di Run (ON→OFF) per spegnere la lavatrice. A questo punto il ciclo si ripete e dopo un'ulteriore pressione di Run (OFF→ON) si ha lo stato di Pending di verifica delle variabili d'interfaccia utente precedentemente descritto.
- ✚ **PAUSE**: È prevista la possibilità della sospensione momentanea dell'esecuzione del programma selezionato nel caso in cui, durante lo svolgimento di una delle fasi, sia premuto il pulsante di Run (ON→OFF). La pausa prevede l'interruzione delle azioni base come l'immissione dell'acqua o il controllo di temperatura se queste sono in svolgimento al reset del pulsante. Un'ulteriore set del pulsante Run (OFF →ON) riattiva l'esecuzione del programma a partire dallo stato in cui era stata freezata. A tal proposito si sfrutta la SFC flag SFCPause di Codesys come approfondito nel paragrafo "Struttura software della soluzione".

2. Struttura software della soluzione:

Per garantire modularità e riusabilità del software stesso, il codice del controllo è organizzato in POU, secondo la standard IEC 61131-3 che definisce l'implementazione del controllo logico su PLC.

Di seguito sono analizzate le POU utilizzate suddivise in ognuna delle 3 tipologie di POU definite dallo standard.

3.1 FUNCTION BLOCKs

➤ Attuatori Generalizzati (GAs)

Sulla base della metodologia di progetto adottata detta degli “Attuatori Generalizzati”, gli Automi di Meccanismo (realizzati come GA) in grado di eseguire le azioni base quando richiesto dall’Automa di Politica, sono implementati mediante Function Block. Essi sono definiti come segue:

A) Identificazione delle azioni base:

NOME IDENTIFICATIVO	DESCRIZIONE	SENSORI	ATTUATORI	TIPOLOGIA
WaterFilling	Immissione acqua nel cestello fino al livello fissato	waterlevel	fillwater	Do-Done
WaterEmptying	Svuotamento acqua dal cestello	waterlevel	emptywater	Do-Done
TemperatureControl	Regolazione della temperatura dell’acqua del cestello a un valore fissato	temperature	hot	Start-Stop
DoorLocking	Blocco dello sportello	bulls_eye_open	bulls_eye_lock	Do-Done
DoorUnlocking	Sblocco dello sportello	bulls_eye_open	bulls_eye_lock	Do-Done
WMDrumMotorON	Accensione motore della lavatrice per un tempo fissato	-	Motor_on	Start-Stop
Soaping	Svuotamento del sapone della vaschetta	soaplevel	emptysoap	Start-Stop

B) Definizione dei GAs:

GA	INPUTS		OUTPUTS			
	PortName	Values	PortName	Values		
WaterManagement_GA (Do-DONE)	High Level interface (to policy)					
	Do_	TRUE	Done	TRUE		
		FALSE		FALSE		
	DoWhat	Do_WaterFilling	failure	WaterIn	WaterOut	
		Do_Emptying		Heat	None	
	Restore	TRUE	flt_case	early	mid	late
		FALSE				
	FillTest	TRUE				
		FALSE				
	Low Level Interface					
	waterlevelPort	waterlevel	State	S_Init	S_Ready	
				S_Busy	S_Fault	
FillLev	100	fillwaterPort	fillwater			
EmptyLev	0	emptywaterPort	emptywater			
TempControl_GA (Start-Stop)	High Level Interface					
	Start	TRUE	State	S_Init	S_Ready	
		FALSE		S_Busy	S_Fault	
	Stop	TRUE	TempOk	TRUE		
		FALSE		FALSE		
	StartWhat	Warm30				
		Warm60				
		Warm90				
	HeatTest	TRUE				
		FALSE				
	Restore	TRUE				

		FALSE			
	Low Level Interface				
	temperaturePort	temperature	hotPort	hot	
	Delta	2			
DoorLocking_GA (Do-Done)	High Level Interface				
	Do_	TRUE	Done	TRUE	
		FALSE		FALSE	
	DoWhat	Do_Locking	State	S_Init	S_Ready
		Do_Unlocking		S_Busy	S_Fault
			OpenDoor	TRUE	
				FALSE	
	Low Level Interface				
	bulls_eye_openPort	bulls_eye_open	bulls_eye_lockPort	bulls_eye_lock	
	DrumMotor_GA (Start-Stop)	High Level Interface			
StartMotor		TRUE	State	S_Init	S_Ready
		FALSE		S_Busy	S_Fault
StopMotor		TRUE			
		FALSE			
Low Level Interface					
			motor_onPort	motor_on	
SoapEmptying_GA (Start-Stop)	High Level Interface				
	StartSoap	TRUE	State	Init	Ready
		FALSE		Busy	Fault
	StopSoap	TRUE	NoSoap	TRUE	
		FALSE		FALSE	
	Low Level Interface				
	soaplevelPort	soaplevelPort	emptysoapPort	emptysoap	

Note importanti sui GA:

- Diagnostica di basso livello per il corretto comportamento tra attuatori e sensori:

La fault Detection relativa ad attuatori e sensori di pertinenza di un GA è incapsulata nel GA stesso. La comunicazione della presenza di un guasto alla politica è garantita in primis dal passaggio ad uno stato di Fault del SFC del GA che ha rilevato un'anomalia. Sono presenti ulteriori variabili di interfaccia di uscita verso la politica per garantire una corretta Isolation del fault, come nel caso del GA WaterManagement_GA dove occorre distinguere i casi di otturazione del tubo di immissione o di scarico dell'acqua (rispettivamente fault di tipo WaterIn o WaterOut).

Un'analisi approfondita sull'implementazione nel progetto di diagnostica e gestione delle anomalie è affrontata nel paragrafo 3.

- Protocollo di handshake tra politica e GA per i GA di tipo Do-Done:

Con lo scopo di evitare attivazione multiple (o corse critiche) di un'azione base viene implementato un set reset alternato di Do e Done da parte rispettivamente di Politica e GA. In particolare, quando la Politica setta il Do di un GA e viene terminata l'azione base di pertinenza il GA setta il Done ma prima di passare dallo stato di Busy a quello di Ready si attende il reset del Do da parte della Politica. A questo punto il GA resetta anche il Done per poi passare al successivo stato di Ready.

- Do_Abort per la pausa del ciclo:

Qualora sia richiesta una pausa del funzionamento secondo le modalità specificate nel primo paragrafo, allora, indipendentemente dall'Automa di Politica (AdP) Child attivo in quel momento, questo verrà sospeso dall'AdP Parent grazie alla Flag SFCPause (i dettagli sulle Politiche implementate sono espressi

nel paragrafo successivo), e sarà attivato un segnale di Do_Abort per sospendere momentaneamente l'operatività di tutti i GA. Alla ripresa del funzionamento tale segnale viene resettato e si prosegue l'esecuzione del programma a partire dallo stesso step in cui si era fermato.

2.2 PROGRAMS

➤ **ParentPolicyAutomata:**

Tale Automa di Politica è rappresentato dal SFC Padre di questo controllo logico che gestisce l'attivazione/sospensione delle Politiche figlie sulla base dello stato di salute della politica in esecuzione o della richiesta di una pausa dall'esecuzione. All'avvio del controllo logico la Politica è inizializzata come Healthy e viene attivato l'SFC relativo alla Politica Nominale.

➤ **ChildPolicyAutomatas:**

A) *Nominal_PA*: è l'SFC che definisce la politica nominale, la quale coordina il comportamento atteso della lavatrice, cioè, esegue un check sugli input ad ogni avvio e se la verifica è andata a buon fine prosegue con il ciclo completo del programma della lavatrice, ovvero, esegue in loop le fasi che compongono il programma fino al suo termine.

B) *WaterInFaulty_PA*: è l'AdP che gestisce l'esecuzione degradata della fase in cui si dovesse verificare l'otturazione del tubo di immissione dell'acqua nel cestello durante il riempimento del cestello stesso ma il livello di acqua già presente consente comunque l'operatività della fase (solo per i casi "mid" e "late" di WaterIn fault, per i dettagli si rimanda al paragrafo seguente).

C) *WaterInFaulty_PA*: è l'AdP che coordina il ciclo completo a freddo nel caso in cui si dovesse verificare la rottura della resistenza per il riscaldamento dell'acqua.


N.B. Maggiori approfondimenti sul partizionamento degli AdP e sulla gestione del coordinamento degli stessi sulla base delle anomalie riscontrate sono riportati nel paragrafo successivo.

➤ **GA_Collector:**

Codice FBD in cui sono definite le istanze dei GA specifiche per questo controllo logico.

➤ **Simulation_Program:**

Codice per la simulazione dell'impianto non controllato.

 **NOTA:** ognuna di questi Program rappresenta un Task (attività) da associare ad ogni tempo di scansione (detto invece "MainTask" nella nomenclatura di Codesys)

3.3 FUNCTIONS:

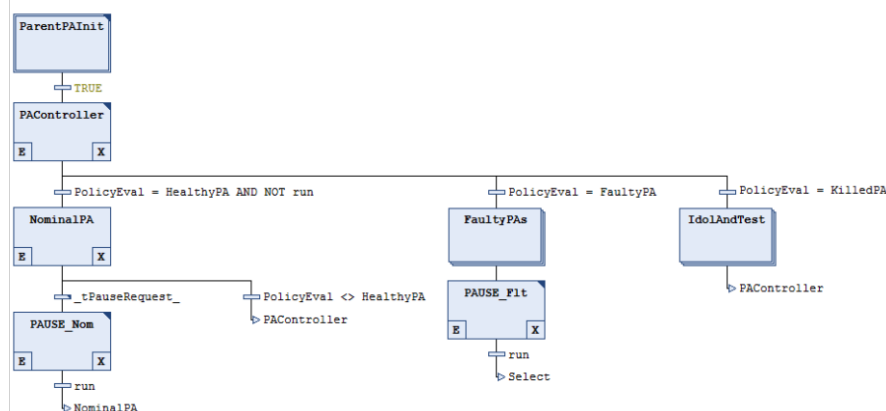
Per garantire una pulizia migliore del codice sono state implementate alcune funzioni da richiamare più volte all'interno delle azioni (*Step Actions*) dei vari SFC, tra queste:

- *WMProgramCheck/WMTempCheck*: verificano che programma e temperatura selezionati dall'utente tramite HMI siano corretti;
- *SetBools*: setta o resetta gruppi di variabili booleane insieme;
- *FaultHMI*: accende una tra le spie luminose di segnalazione del fault in HMI;
- *CheckFault*: verifica quale anomalia si è presentata (Fault Isolation) grazie alla comunicazione delle variabili d'interfaccia di uscita dei GA.

3. Metodo di gestione generalizzata dei fault

Il metodo di gestione dei Fault proposto si basa sull'idea di partizionamento degli SFC degli Automi di Politica (AdP) in più Program distinti in grado di interagire tra loro mediante le variabili SFC Flags generate implicitamente da Codesys, le quali consentono una gestione di tipo pseudo-**Parent/Child** di più SFC. Si hanno dunque più SFC detti "Child" che sono gestiti dalle chiamate di un SFC "Parent" in grado di avviare o arrestare un Children SFC, in particolare mediante i flag SFCInit e SFCPause.

Nel caso specifico di questo progetto si hanno l'AdP Parent (ParentPA) che durante il comportamento nominale del sistema attiva l'AdP Nominale (NominalPA), al contempo però riceve informazioni dai vari GA sullo stato di salute della Politica, la quale può essere valutata come **Healthy, Faulty o Killed**. Sulla base di tale valutazione l'AdP Parent potrà attivare rispettivamente NominalPA, uno tra i due AdP Faulty (HeatFaultyPA o WaterInFaultyPA), oppure eseguire una serie di step per passare allo stato di Idol e di richiesta di manutenzione.



3.1 Diagnostica dei guasti di sensori/attuatori

Come richiesto è implementato nel controllo logico una struttura software aggiuntiva per consentire la diagnostica verso il basso, cioè quella del corretto funzionamento tra attuatori e sensori. In particolare, le anomalie previste sono guasti che compromettono uno (single-fault) o più attuatori contemporaneamente (multiple-faults) tra quelli di immissione dell'acqua, di scarico della stessa o di regolazione della temperatura. La "**Fault Detection**" è incapsulata nei GA, così come una prima forma di gestione locale urgente del guasto. La segnalazione verso l'AdP Parent della presenza di un fault avviene sia mediante la valutazione dello stato della Politica come Healthy, Faulty o Killed sia tramite le variabili di uscita di interfaccia dei GA per dettagliare il guasto riscontrato.

3.2 Gestione dei fault

Una prima forma di gestione immediata dei fault avviene localmente al GA di pertinenza dell'attuatore guasto arrestandone il funzionamento.

A seconda dell'anomalia riscontrata il ciclo nominale di funzionamento della lavatrice subisce poi delle modifiche, in particolare il programma sarà portato a termine in maniera degradata qualora l'entità dell'anomalia lo permetta, oppure l'esecuzione delle fasi verrà immediatamente sospesa:

- A. Guasto alla resistenza: viene ugualmente portato a termine il programma selezionato ma a freddo (si trascura la temperatura impostata, bypassando la regolazione della stessa). Si decide inoltre di abbassare la durata delle fasi del ciclo; perciò, il programma è completato in maniera degradata. Terminato il ciclo si passa in una condizione di idol e di attesa di manutenzione

Il GA di regolazione della temperatura valuta la Politica come Faulty, da cui ParentPA sospende NominalPA, attiva HeatFaultyPA per il proseguo del funzionamento in maniera degradata ed accende il led apposito di segnalazione del fault in HMI.

- B. Guasto allo scarico dell'acqua, l'esecuzione è immediatamente interrotta, il sistema passa in una condizione di idol in attesa di manutenzione (killer-fault). Il GA di gestione del livello dell'acqua valuta la Politica come Killed, ParentPA sospende NominalPA, accende il led di segnalazione del fault in HMI.
- C. Guasto al riempimento dell'acqua: 3 casi possibili a seconda del livello di acqua presente nel cestello nel momento in cui si verifica l'otturazione del tubo di immissione:

- I. $livello\ acqua < 20 \Rightarrow WinFlt_case = early$

Esecuzione sospesa immediatamente e condizione di idol e attesa manutenzione (killer-fault).

- II. $20 \leq livello\ acqua < 70 \Rightarrow WinFlt_case = mid$

Esecuzione degradata della sola fase in corso del programma, con una durata superiore e con temperatura fissata a 30 gradi per sicurezza. Vista l'impossibilità di riempire nuovamente il cestello, terminata la suddetta fase si passa in una condizione di idol di attesa di manutenzione.


NOTA: qualora la fase da portare a compimento richieda l'utilizzo del sapone questo non sarà utilizzato perché in ogni caso il risciacquo finale non viene eseguito.


- III. $70 < livello\ acqua \leq 100 \Rightarrow WinFlt_case = late$

Svolgimento della sola fase corrente in maniera identica al funzionamento nominale, se la fase è di lavaggio (richiede sapone), allora la durata è superiore per permettere di lavare bene e viene svuotato solo una parte del sapone.

Nel caso I il GA di gestione del livello dell'acqua valuta la Politica come Killed, nei casi II e III la Politica è valutata come Faulty. In tutti i casi ParentPA accende il led di segnalazione del fault in HMI e passa l'esecuzione al SFC predisposto alla gestione del fault come già descritto.

IMPORTANTE: Al termine di tutte le forme di gestione suddette occorre sbloccare la chiusura dell'oblò per permettere l'apertura dello sportello.

 **IdolAndTest**: Una volta completata l'esecuzione degradata, se possibile, oppure subito, nel caso di un killer-fault, il ParentPA sospende tutti i ChildPA ed esegue un Macro Step che prevede lo **sblocco dello sportello** della lavatrice e il passaggio in una condizione di **idol**, cioè di attesa di un intervento da parte di un operatore esterno con l'obiettivo di ripristinare il funzionamento corretto del sistema risolvendo i guasti degli attuatori malfunzionanti. Nonostante nella realtà ciò non sia possibile, si **ipotizza** che tale intervento avvenga in tempi molto ridotti e senza togliere l'alimentazione alla lavatrice e dei suoi attuatori. Durante questa fase, in simulazione evidenziata dal lampeggiamento dei led corrispondenti ai guasti presenti, si può pensare di spegnere tramite HMI gli switch che simulano i fault. Terminato l'intervento viene eseguito un **test di corretto funzionamento** del dispositivo riparato, cioè a seconda che si fosse verificato un fault singolo o più fault multipli, si esegue il test di uno o più attuatori generalizzati in sequenza e delle rispettive azioni base su cui si era verificata l'anomalia. Se il test di tutte le azioni è andato a buon fine la Politica sarà valutata come Healthy e ParentPA potrà attivare nuovamente NominalPA da cui si avrà il comportamento nominale e sarà possibile una nuova richiesta di avvio della lavatrice secondo le modalità specificate precedentemente.

 **Gestione fault multipli**: Se durante l'esecuzione degradata di una fase del programma impostato dovuta ad una prima anomalia riscontrata si verifica un altro fault aggiuntivo allora questo viene gestito allo stesso modo secondo gli stessi principi non appena rilevato dal GA di pertinenza. A seconda che i fault multipli permettano un funzionamento degradato o meno si potrà assistere a fasi di lavorazione ulteriormente degradate oppure sospese per la presenza di un killer-fault.