Macchine sequenziali in sicurezza: logiche applicative in ambito ferroviario

Sequential safety machines: application logic in the railway sector

Dott. Ing. Gabriele PUPOLIN[(*)]

Sommario - Le macchine sequenziali sono macchine dotate di un rudimentale "pensiero artificiale" costituito dal loro "stato interno" o memoria [1]. Questa intelligenza artificiale può essere di aiuto nelle attività svolte dall'uomo in ambienti tecnici in cui siano presenti elevati rischi. Definiremo ambienti tecnici con elevati rischi quelli in cui gli errori nella manipolazione di organi e attrezzature possono arrecare gravi danni a cose o a persone.

Un campo di attività in cui gli errori umani possono avere conseguenze gravi è rappresentato dalla gestione della circolazione treni. Ciò per le velocità e le masse in gioco nonché per i notevoli spazi di frenatura necessari per fermare il treno.

Sin dagli inizi si è sentita la necessità di regolamentare l'operatività degli addetti alla circolazione treni con precise procedure da rispettare. Via via tali procedure sono state sostituite con sistemi meccanici, elettromeccanici ed elettronici liberando gli operatori addetti alla gestione della circolazione treni dalle responsabilità connesse al controllo di condizioni impiantistiche. Tali sistemi (di ausilio agli operatori), su cui ricade la responsabilità di parte dei controlli legati alla sicurezza della circolazione treni, sono definiti apparati di sicurezza.

Gli apparati di sicurezza sono macchine sequenziali complesse che si possono disaggregare in macchine sequenziali più semplici tra loro interagenti. Lo studio di tali apparati rappresenta una disciplina tipicamente ferroviaria; il loro studio in termini di macchine sequenziali permette di avere un approccio sistemico nei confronti di tale disciplina.

Dare forma sistemica allo studio degli apparati di sicurezza permette di intervenire nei confronti degli stessi con maggior capacità di analisi e sintesi sia in fase di loro progettazione che in fase di loro verifica.

Questo articolo si propone di rappresentare alcune tipologie di apparati di sicurezza in uso nella Rete Ferroviaria Italiana con dei modelli di macchine sequenziali;

Summary - *Sequential machines are machines equipped with rudimentary "artificial thinking" formed by their "internal state" or memory [1]. This artificial intelligence can help in activities carried out by man in technical environments where there are high risks. We shall define technical environments with high risks those where errors in the handling of devices and equipment may cause serious damage or injury to persons.*

Train traffic management represents a field of activity where human errors can have serious consequences. This is due to speed and masses at stake as well as the considerable braking spaces required to stop the train.

From the very beginning the need was felt to regulate the operation of the persons in charge of train circulation with precise procedures to be followed. Gradually such procedures have been replaced with mechanical, electromechanical and electronic systems leaving traffic management train operators free from the responsibility related to the control of plant conditions. Such systems (supporting operators), on which the responsibility of part of the train traffic safety-related controls rests, are defined safety devices.

Safety devices are complex sequential machines that can be broken down in easier sequential machines interacting between each other. The study of such devices represents a typically rail procedure; their study in terms of sequential machines enables a systematic approach with respect to that discipline.

The systemic shaping of the study of safety devices allows intervening on the same with greater analysis and synthesis capacity, both during their design stage and their verification.

This article aims to represent certain types of safety equipment in use on the Italian Railway Network with sequential machine models; in such examination the ability to maintain adequate levels of security for these machines will be assessed also in case of possible faults involving them.

(*) Dirigente RFI a r.

(*) *RFI a r. Manager.*

in tale disamina saranno valutate le capacità di mantenere adeguati livelli di sicurezza da parte di tali macchine anche in caso di guasti che le possano interessare.

1. Premessa

Come macchina sequenziale a Stati Finiti o Automa a Stati Finiti (ASF o FSA – Finite State Automata) si intende un modello in grado di descrivere un sistema caratterizzato dalle seguenti specificità:

– evoluzione nel tempo;

– insiemi di variabili discrete e finite.

Una ulteriore specificità del sistema potrebbe esser rappresentata dall'evoluzione deterministica oppure no delle sue variabili.

In questo articolo sarà presa in considerazione una macchina sequenziale a stati finiti deterministica [2]. L'evoluzione di una generica macchina sequenziale è rappresentabile con tre insiemi di variabili;

– variabili di ingresso $(I_i)_n$;

– variabili di stato $(S_j)_n$;

– variabili di uscita $(O_k)_n$;

e due leggi di composizione esterna:

– Γ_1 avente dominio nel prodotto cartesiano[1] tra le variabili di ingresso e le variabili di stato e codominio nelle variabili di stato:

$$(I)_n \, \Gamma_1 \, (S)_n = (S)_{n+1}$$

– Γ_2 avente codominio nelle variabili di uscita e dominio o nelle variabili di stato o nel prodotto cartesiano tra variabili di ingresso e le variabili di stato:

$$(I)_n \, \Gamma_2 \, (S)_n = (O)_{n+1}$$

L'indice *n* delle variabili rappresenta il passo *n* dell'evoluzione della macchina sequenziale a stati finiti.

Tra le macchine sequenziali a stati finiti deterministiche definiremo "macchine sequenziali in sicurezza" quelle macchine la cui evoluzione sia finalizzata a realizzare sequenze procedurali atte a far operare all'interno di un sistema persone o macchine mantenendo la sicurezza delle stesse.

2. Descrizione di una generica macchina sequenziale in sicurezza

La procedura in grado di descrivere la gestione di un'attività in sicurezza all'interno di un sistema è la seguente:

[1] Dati due insiemi, il loro prodotto cartesiano è l'insieme di tutte le coppie ordinate di cui il primo elemento viene dal primo insieme e il secondo dal secondo insieme. Consente di trattare sulla base del postulato definitorio degli insiemi anche altri legami tra insiemi, tra cui in particolare il legame funzionale oggetto della presente trattazione.

1. Introduction

A Finite State machine or Finite State Automata sequential machine (ASF or FSA – Finite State Automata-) is understood as a model capable of describing a system characterised by the following peculiarities:

– *evolution over time;*

– *sets of discrete and finite variables.*

Another characteristic of the system may be represented by the deterministic evolution or not of its variables.

This article will consider a sequential deterministic finite-state machine [2]. The evolution of a generic sequential machine can be represented with three sets of variables:

– *input variables* $(I_i)_n$;

– *status variables* $(S_j)_n$;

– *output variables* $(O_k)_n$;

and two external composition laws:

– Γ_1 *having domain in the Cartesian product*[1] *between input variables and state variables and codomain in the state variables:*

$$(I)_n \, \Gamma_1 \, (S)_n = (S)_{n+1}$$

– Γ_2 *with codomain in the output variables and domain or in the state variables or Cartesian product between input variables and state variables:*

$$(I)_n \, \Gamma_2 \, (S)_n = (O)_{n+1}$$

Index n of the variables represents step n in the evolution of the finite state sequential machine.

Among the deterministic finite state sequential machines we shall define "sequential safety machines" those machines whose evolution is aimed to achieve procedural sequences designed to allow persons or machinery to operate within a system maintaining the safety of the same.

2. Description of a generic sequential safety machine

The procedure that can describe the management of a task safely within a system is as follows:

1) *normal system operating condition (or rest);*

2) *manoeuvre of bodies able to delimit a safe area or provide a secure path within the system;*

3) *collection of position controls of devices handled;*

4) *locking of devices moved so that they are manoeuvrable only after having removed the lock;*

[1] *Given two sets, their Cartesian product is the set of all ordered pairs whose first element is from the first set and the second from the second set. It allows dealing also with other connections between sets, on the basis of the defining hypothesis of the sets, among which in particular the functional relationship involved in this dissertation.*

1) stato di funzionamento normale (o di riposo) del sistema;
2) manovra di organi in grado di delimitare un'area sicura o predisporre un percorso sicuro all'interno del sistema;
3) raccolta dei controlli di posizione degli organi movimentati;
4) bloccaggio degli organi movimentati in maniera che non siano manovrabili se non dopo aver rimosso il bloccaggio;
5) accesso all'area messa in condizioni di sicurezza;
6) uscita dall'area messa in condizione di sicurezza;
7) rimozione del bloccaggio degli organi;
8) manovra degli organi con ripristino delle condizioni di funzionamento normale (o di riposo) del sistema.

La gestione degli organi deputati alla delimitazione dell'area da porre in sicurezza, presupponendo la loro condizione in due soli stati (aperto, cui sarà attribuito il valore logico "0", o chiuso, cui sarà attribuito il valore logico "1"), può esser così riassunta:

– stato di riposo: controllo dell'organo in posizione "1";
– comando di manovra; organo in movimento;
– ottenimento controllo di esecuzione manovra completata: organo in posizione "0"; Bloccaggio dell'organo nella nuova posizione: organo in posizione "0"; Rimozione bloccaggio organo: organo in posizione "0";
– rimozione comando di manovra: organo in movimento;
– ritorno dell'organo nello stato di riposo: organo in posizione "1".

La gestione può inoltre prevedere che a seguito di ogni movimentazione dell'organo ci sia un solo intervento in sicurezza all'interno del sistema; ciò richiederà un percorso ciclico (da controllare) dell'evoluzione dell'automa che rappresenterà la gestione dell'organo.

Possiamo rappresentare l'automa con una macchina sequenziale a quattro stati come rappresentato in fig. 1.

Una realizzazione fisica di tale automa può esser fatta con due Flip Flop tipo D[2] come rappresentato in fig. 2.

Nel circuito di fig. 2 CC rappresenta il controllo della nuova posizione raggiunta dall'organo movimentato e CB rappresenta il controllo della posizione di un elemento di bloccaggio sull'organo movimentato. A queste due varia-

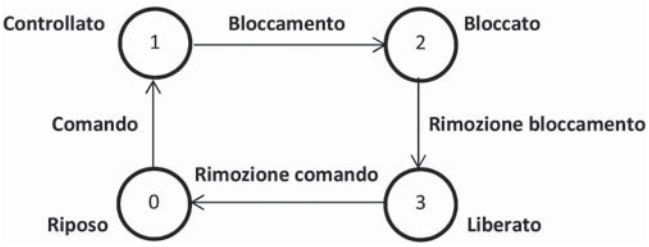

Fig. 1 - Diagramma degli stati della macchina sequenziale rappresentante la movimentazione degli organi.
Fig. 1 - Sequential machine states diagram representing the movement of units.

5) *access to the area placed in safe conditions;*
6) *exit from the area placed in safe conditions;*
7) *removal of the lock of the devices;*
8) *operation of devices with recovery of normal system operating conditions (or rest).*

The management of the units responsible for redlining the safety area, assuming their condition in only two statuses (open, to which the logical value "0" will be assigned, or closed, to which the logical value "1" will be assigned), can be summarised as follows:

– *standby: control of the unit in position "1";*
– *manoeuvre command: moving unit;*
– *obtaining manoeuvre completed control – unit in position "0"; Locking of the unit in the new position – unit in position "0 "; Removal of locking unit – unit in position " 0 ";*
– *removal of manoeuvre command: moving unit;*
– *return of the unit in the idle status: unit in position "1".*

The management may also provide that following every unit handling, there is only one safety intervention within the system; this will require a cyclic path (to control) of the evolution of the automaton that will represent the management of the unit.

We can represent the automaton with a sequential machine in four states as shown in fig. 1.

A physical realisation of this automaton can be made with two D type Flip Flops[2], as shown in fig. 2.

In the circuit of fig. 2 CC is the control of the new position achieved by the moved unit and CB is the control of the

[2] I Flip Flop, o multivibratori bistabili, rappresentano il più semplice circuito sequenziale in grado di memorizzare un evento (un circuito sequenziale è un circuito in cui le uscite dipendono dalla sequenza degli ingressi che si sono succeduti). Presentano in uscita due soli valori di tensione stabili associabili ai livelli logici "0" e "1". Il Flip Flop tipo D (data) presenta un ingresso per il dato (D) e un ingresso per il sincronismo (Clock). All'attivarsi del comando di sincronismo, il dato presente in D transita all'uscita Q del Flip Flop e vi permane sino al nuovo Clock.

[2] *Flip Flops, or bistable multi-vibrators, represent the simplest sequential circuit capable of storing an event (a sequential circuit is a circuit in which the outputs depend on the sequence of successive inputs).They only have two stable tension values outputs that can be associated with logical levels "0" and "1". The D type Flip Flop (data) has an input for the data (D) and an input for the synchronism (Clock). As the synchronism command is enabled, the data in D transits at output Q of the Flip Flop and remains there until the new Clock.*

bili esterne vanno aggiunte le variabili interne Q_1 e Q_2 rappresentanti le uscite dei due Flip Flop.

Esaminiamo brevemente il comportamento di tale macchina sequenziale in sicurezza.

Stato "0". A riposo i due Flip Flop presentano le loro uscite a valore "0" in quanto nessuna delle uscite dei circuiti AND risulta a valore logico "1". Lo stato "0" è quindi caratterizzato dal settaggio delle due variabili interne ai seguenti valori logici:

$$Q_1 = \text{“0”}; Q_2 = \text{“0”}$$

Operato il comando e ottenuto il controllo di posizione dell'organo movimentato, la variabile *CC* assume il valore logico "1" mandando l'uscita dell'AND di sinistra in fig. 2 al valore logico "1". Con il clock il Flip Flop 1 transita con la sua uscita Q_1 al valore logico "1". Il Flip Flop 2 permane con Q_2 a valore logico "0".

La macchina sequenziale raggiunge lo stato "1" che risulta caratterizzato dal settaggio delle due variabili interne ai seguenti valori logici:

$$Q_1 = \text{“1”}; Q_2 = \text{“0”}$$

Manipolato il bloccamento dell'organo ed ottenuto il controllo di posizione dell'elemento bloccante, l'AND centrale di fig. 2 presenta uscita a valore logico "1". Intervenendo tale AND sugli ingressi di ambedue i Flip Flop, all'attivarsi del clock ambedue i Flip Flop presenteranno le loro uscite Q a valore logico "1".

La macchina sequenziale raggiunge lo stato "2" che risulta caratterizzato dal settaggio delle due variabili interne ai seguenti valori logici:

$$Q_1 = \text{“1”}; Q_2 = \text{“1”}$$

Lo stato "2" della macchina sequenziale rappresenta lo stato in cui è possibile accedere in sicurezza all'interno del sistema; esso pertanto abiliterà un'uscita che permetterà l'accesso all'interno del sistema.

Per tutto il periodo in cui esisterà l'accesso all'interno del sistema sarà impossibile rimuovere dalla sua posizione l'elemento che ha operato il bloccamento dell'organo.

Completata l'operazione all'interno del sistema e ripristinato il suo stato di non accessibilità, sarà possibile rimuovere l'elemento bloccante dell'organo movimentato.

Con il ritorno della variabile *CB* a valore logico "0" si avrà la disposizione al valore logico "1" per il solo AND di destra di fig. 2. Il Flip Flop 1 farà transitare la sua uscita Q_1 a valore logico "0"; il Flip Flp 2 permarrà con la sua uscita Q_2 a valore logico "1".

La macchina sequenziale raggiunge lo stato "3" che risulta caratterizzato dal settaggio delle due variabili interne ai seguenti valori logici:

$$Q_1 = \text{“0”}; Q_2 = \text{“1”}$$

Con la rimozione del comando e ritorno a livello logico "0" della variabile *CC* nessuna delle uscite dei circuiti

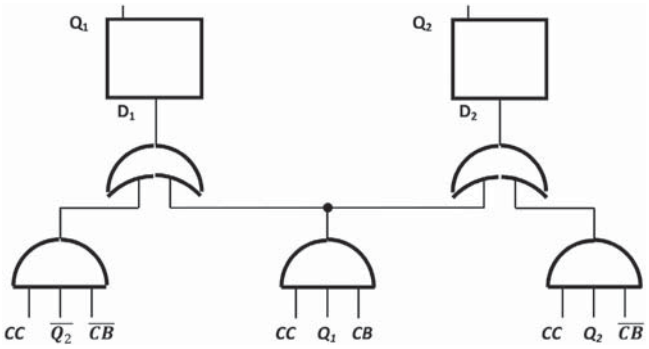

Fig. 2 - Circuito con Flip Flop tipo D realizzante una macchina sequenziale in sicurezza.

Fig. 2 - Circuit with D type flip flop creating a sequential safety machine.

position of a locking piece on the moved unit. These two external variables must be added to the internal variables Q_1 and Q_2 representing the outputs of the two Flip Flops.

Let us briefly examine the behaviour of such sequential safety machine.

State "0". At rest, the two Flip Flops have their outputs with value "0" since no circuit AND outputs have logical value "1". The "0" state is therefore characterised by the setting of the two internal variables to the following logical values:

$$Q_1 = \text{“0”}; Q_2 = \text{“0”}$$

Having operated the command and obtained the position control of the moved unit, the CC variable takes logical value "1" by sending the left AND output in fig. 2 to logical value "1". With the clock Flip Flop 1 passes with its Q_1 output to logical value "1". Flip Flop 2 continues with Q_2 with logical value "0". The sequential machine reaches state "1" which is characterised by the setting of the two internal variables to the following logical values:

$$Q_1 = \text{“1”}; Q_2 = \text{“0”}$$

After manipulating the locking of the unit and gained the position control of the locking element, the central AND in fig. 2 has logical value output "1". As such AND intervenes on the inputs of both Flip Flops, as the clock activates, both Flip Flops will have their Q outputs with logical value "1".

The sequential machine reaches state "2" that is characterised by the setting of the two internal variables with the following logical values:

$$Q_1 = \text{“1”}; Q_2 = \text{“1”}$$

State "2" of the sequential machine represents the state where the system can be safely accessed internally; it will therefore enable an output that will allow access inside the system.

Throughout the period during which there will be access within the system, it will be impossible to remove the locking unit from its position.

logici AND assume valore logico "1" e al successivo clock anche Q_2 ritornerà a valore logico "0".

La macchina sequenziale ritorna allo stato "0" completando il suo percorso ciclico.

Il diagramma temporale di evoluzione dei due Flip Flop è riportato in fig. 3.

La macchina sequenziale appena descritta dallo stato "1" può ritornare nello stato "0" con la rimozione del comando dell'organo ed il ritorno a valore logico "0" della variabile *CC*. Per come sono strutturati fisicamente l'organo da movimentare e il suo elemento bloccante, la presenza della variabile *CB* a valore logico "1" impedisce di poter avere la variabile *CC* a valore logico "0". La condizione *CC* = "0" con *CB* = "1" non viene presa in esame nel circuito di Fig. 2 in quanto fisicamente non realizzabile.

Tale condizione potrebbe comunque essere frutto di una condizione di guasto nei circuiti elettrici. Per parare questa situazione basta che variabile *CB* in ingresso ai circuiti logici di fig. 2 rappresenti l'uscita di un AND logico tra le variabili fisiche *CC* (con funzione di Enable) e *CB'* proveniente dal campo. Ulteriore garanzia del corretto funzionamento della macchina sequenziale di fig. 2 può esser ottenuta con il controllo della sequenza ciclica degli ingressi e degli stati rappresentati dalle uscite dei Flip Flop (questa soluzione comporta il dover memorizzare una stringa di bit costituita dall'ingresso che ha causato il passaggio allo stato 1, dallo stato 1, dall'ingresso che ha causato il transito allo stato 2 e dallo stato 2; il corretto contenuto di tale striga va verificato prima di abilitare l'uscita).

Un'applicazione della macchina descritta in fig. 2 può esser costituita dalla procedura prevista per l'accesso all'interno di un box contenente apparecchiature elettriche in tensione. Gli organi da manovrare saranno i sezionatori elettrici che aperti disalimenteranno le apparecchiature elettriche interne al box. Gli elementi che attuano i bloccamenti dei sezionatori elettrici potranno essere degli slot che, azionati, impediranno al sezionatore aperto di essere chiuso. Arrivati allo stato di bloccato, si attiverà un'uscita che permetterà l'apertura di un cancello di accesso all'in-

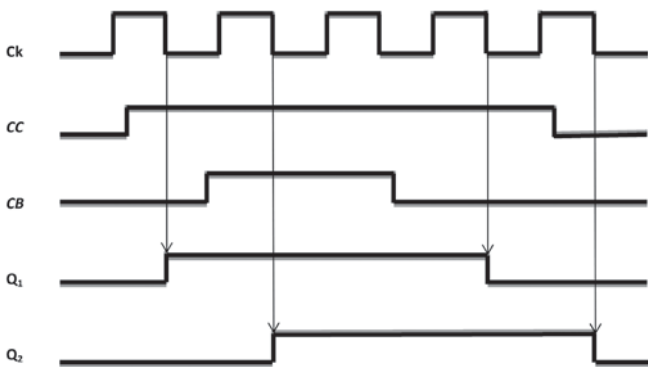

Fig. 3 - Evoluzione temporale della macchina sequenziale.
Fig. 3 - Time evolution of the sequential machine.

Upon completion of the operation within the system and after restoring its non-accessibility state, the element locking the moved unit can be removed.

As variable CB returns to logical value "0", logical value "1" is provided only for the right AND in fig. 2. Flip Flop 1 will pass its Q_1 output to logical value "0"; Flip Flop 2 will remain with its Q_2 output with logical value "1".

The sequential machine reaches state "3" that is characterised by the setting of the two internal variables with the following logical values:

$$Q_1 = \text{"0"};\ Q_2 = \text{"1"}$$

With the removal of the command and return of variable "CC" to logic level 0, none of the outputs of the AND logic circuits assumes logical value "1" and at the next clock Q_2 also returns to logical value "0".

The sequential machine returns to state "0" by completing its cyclical path.

The timing diagram of the evolution of the two Flip Flops is shown in fig. 3.

The sequential machine described above can return from state "1" to state "0" with the removal of the command of the unit and the return to logical value "0" of the CC variable. Due to the physical structure of the unit to be moved and its locking element, the presence of variable CB with logical value "1" prevents having variable CC with logical value "0". The condition CC = "0" with CB = "1" is not taken into consideration in the circuit of Fig. 2 as it is physically not feasible.

This condition may be the result of a fault condition in the electric circuits. To parry this situation it is sufficient that input variable CB in the logic circuits in fig. 2 represents the output of a logical AND between the CC physical variables (with Enable function) and CB' from the field. A further guarantee of the proper functioning of the sequential machine in fig. 2 can be obtained by controlling the cyclic sequence of inputs and states represented by the Flip Flop outputs (this involves having to memorise a bit string that consists of the input that caused passing to state 1, from state 1, from the input that caused passing to state 2 and from state 2; the proper contents of that string must be verified before enabling the output).

An application of the machine described in fig. 2 can be formed by the procedure laid down for accessing inside a box that contains live electrical equipment. The units to be manoeuvred will be the electrical disconnectors that once opened will disconnect the electrical equipment inside the box. The elements that actuate the electrical isolator locks can be slots that once operated, will prevent the open disconnect switch being closed. Once in the locked state, an output will be activated that will allow the opening of an access gate inside the box. Opening this gate (loss of closure control) will prevent the movement of the slot until the gate is closed, creating a locking of the locking element of the unit (the opening and closing of the gate will also be handled by the sequential machine through a cycle). After

terno del box. L'apertura di questo cancello (perdita del controllo di chiusura) impedirà il movimento dello slot sinché il cancello non sarà richiuso, costituendo un bloccamento dell'elemento bloccante l'organo (l'apertura e la chiusura del cancello saranno gestite anch'esse da macchina sequenziale attraverso un ciclo). Richiuso il cancello sarà possibile azionare lo slot liberando la manovra del sezionatore che potrà essere successivamente chiuso riportando il sistema box nello stato iniziale (fig. 4).

3. Automatizzazione del percorso ciclico delle macchine in sicurezza

La procedura esaminata nel precedente punto richiede l'intervento da parte dell'operatore in più momenti distinti:

- per il comando di movimentazione dell'organo (nell'esempio apertura del sezionatore);
- per il comando dell'elemento bloccante l'organo (nell'esempio movimentazione dello slot);
- per l'attivazione di operazioni connesse all'abilitazione dell'uscita (nell'esempio apertura cancello);
- per la chiusura di operazioni connesse all'abilitazione dell'uscita (nell'esempio chiusura cancello);
- per la rimozione del comando dell'elemento bloccante l'organo (nell'esempio ripristino posizione iniziale dello slot);
- per la rimozione del comando di movimentazione dell'organo (nell'esempio chiusura sezionatore).

Per migliorare l'impegno dell'operatore si possono prendere in considerazione alcune automatizzazioni.

Qualora, secondo le procedure, al movimento dell'organo debba seguire sempre il suo bloccaggio, si può automatizzare la seconda operazione senza alcun intervento da parte dell'operatore. Ne segue che il comando dell'organo comporta, oltre al suo controllo e quindi il passaggio allo stato "1", anche il suo bloccaggio e il controllo dell'elemento di bloccaggio con automatico passaggio allo stato "2". Analogamente si può fare per la rimozione del comando dell'organo. In questo caso la rimozione del comando agirebbe in un primo momento sull'elemento di bloccaggio, liberando l'organo, e successivamente sull'organo stesso. Questo tipo di automatizzazione richiede ulteriori considerazioni che saranno esposte successivamente. In particolare, come nell'esempio in cui l'uscita della macchina sequenziale nello stato "2" abilitava l'apertura del cancello e questa apertura a sua volta bloccava l'elemento di bloccaggio dell'organo, l'automatismo deve mantenere le condizioni di sicurezza previste per l'accesso all'interno del sistema mettendo in campo adeguati vincoli.

L'automatizzazione del bloccaggio dell'organo comporta quindi a dover comprendere nella macchina sequenziale in sicurezza anche le parti abilitate al movimento dall'uscita della stessa Macchina sequenziale (quindi il cancello e i suoi controlli nel nostro esempio).

closing the gate, the slot can be operated by freeing the disconnector that can be subsequently closed by placing the box system back to the initial state (fig. 4).

3. Automation of the cyclic path of safety machines

The procedure discussed in the previous paragraph requires the intervention of an operator in several different times:

- *to control movement of the unit (in the example the disconnect switch opening);*
- *to command the locking element of the unit (in this example slot handling);*
- *to activate operations related to enabling the output (gate opening example);*
- *for closing operations related to enabling of the output (gate closing example);*
- *for removal of the blocking element command organ (in the example restoration of the initial position of the slot);*
- *for removal of the handling command of the unit (in the example disconnector closure).*

To enhance the effort of the operator some automation may be considered.

Where, in accordance with the procedures, movement of the unit should always be followed by its locking, the second operation can be automated without any operator intervention. It follows that the command of the unit involves, in addition to its control and therefore transit to state "1", its locking and the control of the locking element with automatic passage to state "2". Similarly this can be done to remove the command of the unit. In this case the removal of the command would act first on the locking element, freeing the unit, and then on the unit itself. This type of automation requires additional considerations that will be presented later. In particular, as in the example where the output of the sequential machine in state "2" enabled the opening of the gate and this opening in turn blocked the locking of the unit, the automatism must maintain the security conditions required for access within the system using appropriate constraints.

Automation of the locking of the unit involves having to include also the units enabled for the movement from the output of the same sequential Machine in the sequential

Fig. 4 - Manovra e bloccaggio di un sezionatore.
Fig. 4 - Manoeuvre and locking of a disconnector.

Con l'automatizzazione del bloccaggio dell'organo gli stati "1" e "3" diventano stati di transito che la macchina sequenziale percorre in maniera automatica. Di fatto abbiamo una macchina a due stati (libero e bloccato) anziché a quattro stati.

In questa descrizione non vengono presi in considerazione i fine corsa di movimento dell'organo e la logica che li governa.

In fig. 5 è rappresentata una macchina sequenziale a due stati, per realizzare la quale basta un singolo Flip Flop.

4. Efficienza di gestione di una macchina sequenziale in sicurezza

Oltre all'automatizzazione del bloccamento si possono prendere in considerazione altre soluzioni per migliorare la gestione della macchina sequenziale in sicurezza da parte dell'operatore.

Qualora l'operatore debba gestire un numeroso insieme di macchine sequenziali in sicurezza e il movimento dei loro organi richieda un tempo non breve, la restituzione del controllo di posizione può avvenire in tempo alquanto differito rispetto l'istante in cui è stato impartito il comando. Può risultare pertanto utile dare informazione all'operatore del corretto comando impartito e distoglierlo dall'attesa di ottenere il controllo.

Questa soluzione richiederebbe l'introduzione di un ulteriore stato tra lo stato "0" di riposo e lo stato "1" di controllato della macchina sequenziale in sicurezza. Tale stato lo definiremo con il termine di comandato. Per evitare l'introduzione di un ulteriore Flip Flop, necessario alla realizzazione di una macchina sequenziale di cinque stati, qualora esista l'automatizzazione del passaggio dallo stato di controllato allo stato di bloccato, lo stato di comandato può sostituire lo stato di controllato realizzando una macchina sequenziale sempre a quattro stati che differisce dalla macchina sequenziale di fig. 1 solo per il termine che contraddistingue lo stato "1" (comandato) (fig. 6).

La realizzazione della macchina sequenziale con due Flip Flop non differisce alquanto dalla realizzazione presentata in fig. 2, venendo modificata solo la variabile esterna *CC* nell'AND di sinistra con una nuova variabile *Cs* che definiremo comando stabilizzato (fig. 7).

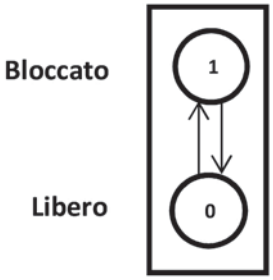

Fig. 5 - Macchina a due stati.
Fig. 5 - Two-state machine.

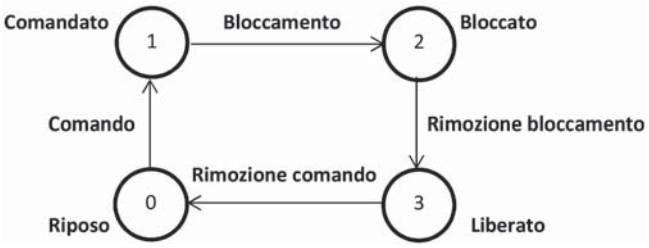

Fig. 6 - Diagramma degli stati della macchina sequenziale con lo stato di "comandato".
Fig. 6 - Sequential machine states diagram with "commanded" state.

safety machine (hence the gate and its controls in our example).

By automating the locking of the unit states "1" and "3" become transit states that the sequential machine runs automatically. In fact we have a two-state machine (free and locked) instead of a four-state one.

The limit movement switches of the unit and the logic that governs them are not taken into account in this description.

Fig. 5 shows a sequential machine in two states, for which a single Flip Flop is required for its realisation.

4. Efficiency of a sequential safety machine

In addition to automating the locking other solutions to improve the management of sequential safety machines by the operator can be considered.

Should the operator need to manage a large set of sequential machines safely and the movement of their units require not a short time, return of the position control can be somewhat delayed in time than the time at which the command was given. It can therefore be useful to give information to the operator regarding the correct command given and distract him from waiting to gain control.

This solution would require the introduction of an additional state between idle state "0" and controlled state "1" of the sequential machine safely. This state will be defined with the term commanded.

To avoid introducing a further Flip Flop, necessary for the realisation of a sequential machine in five states, where there is automation of the passage from the controlled state to the locked state, the commanded status can replace the controlled state by creating a sequential machine in four states that differs from the sequential machine in fig. 1 only for the term that distinguishes state "1" (commanded) (fig. 6).

The realisation of the sequential machine with two Flip Flops does not differ somewhat from the realisation presented in fig. 2, as only the external variable CC is changed in the left AND with a new variable Cs that we shall define stabilised command (fig. 7).

La variabile Cs rappresenta la certezza per l'operatore che il comando è stato correttamente impartito e si resta in attesa si realizzino le condizioni per transitare allo stato "2".

5. Macchine sequenziali in sicurezza complesse

Nell'esempio visto al punto 3, si è esaminata una macchina sequenziale in sicurezza il cui fine era la gestione dell'apertura e della chiusura di un sezionatore.

Prendiamo ora in considerazione l'accesso di una persona all'interno di un box contenente apparecchiature elettriche normalmente alimentate. Dovremmo esaminare lo stato di aperto o chiuso del cancello di accesso al box in funzione dell'apertura di tutti i sezionatori che possono alimentare una qualsiasi apparecchiatura elettrica interna al box. Sia questa operazione automatizzata al massimo assolvendo l'operatore dalle incombenze di manovra di ogni singolo sezionatore. Per realizzare tale automatizzazione dovremmo disporre di una macchina sequenziale complessa scindibile in tre tipologie di macchine sequenziali semplici.

La prima tipologia di macchine sequenziali semplici è costituita dalle macchine sequenziali adibite alla messa in sicurezza dell'area (nel nostro caso le macchine sequenziali legate alla manovra dei sezionatori);

– la seconda tipologia di macchine sequenziali semplici è costituita dalle macchine sequenziali adibite alla manovra degli organi di uscita (nel nostro caso la macchina sequenziale di gestione del cancello);
– la terza tipologia di macchine sequenziali semplici è costituita dalle macchine sequenziali di gestione delle due prime tipologie di macchine sequenziali (a tali macchine sequenziali assegneremo il nome di macchine sequenziali di macro funzione).

Nel caso in esame la procedura che la macchina sequenziale di macro funzione dovrà realizzare sarà la seguente:

– *stato di riposo*: box alimentato dai sezionatori;
– *stato di comandato*: esecuzione da parte dell'operatore del comando di richiesta apertura cancello. Tale richiesta attiverà la manovra di apertura di tutti i sezionatori afferenti al box. Ogni sezionatore sarà gestito da una propria macchina sequenziale in sicurezza del tipo di quella vista in fig. 5. All'operatore perverrà una segnalazione che il comando è stato impartito correttamente;
– *stato di bloccato*: restituzione automatica del controllo di apertura e del bloccaggio di tutti i sezionatori. Il cumulo dei controlli di bloccaggio in apertura dei sezionatori (AND dei loro controlli) opera il bloccaggio della macchina sequenziale di macro funzione e l'attivazione della sua uscita. Quest'ultima interviene sulla macchina sequenziale semplice che gestisce l'apertura del cancello (macchina sequenziale a quattro stati) che passa dallo stato di riposo allo stato di controllato (in

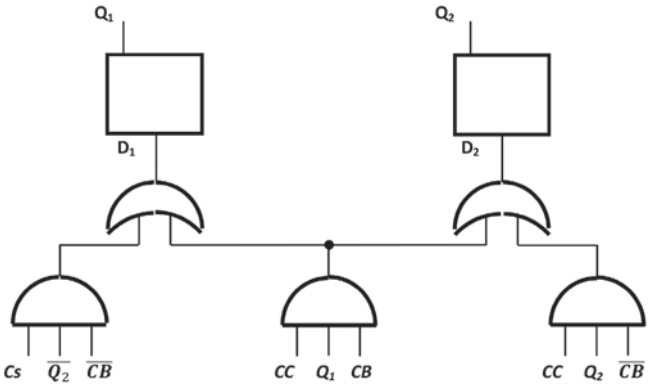

Fig. 7 - Circuito con Flip Flop tipo D realizzante una macchina sequenziale in sicurezza.

Fig. 7 - Circuit with D Type Flip Flop realising a sequential safety machine.

The variable Cs represents the certainty to the operator that the command has been correctly given and pending the realisation of the conditions to pass to state "2".

5. Complex sequential safety machines

In the example seen in point 3, a sequential safety machine was examined whose purpose was the management of the opening and closing of a disconnector.

Let us now consider access by a person inside a box containing electrical equipment powered normally. We should examine the status of open or closed of the access gate to the box according to the opening of all disconnectors that can power any electrical equipment inside the box. Be this operation fully automated discharging the operator from manoeuvre obligations of each individual disconnector. To achieve this automation we should have a complex sequential machine separable into three types of simple sequential machines.

The first type of simple sequential machines consists of sequential machines used for securing the area (in our case the sequential machines related to the manoeuvre of the disconnectors);

– *the second type of simple sequential machines consists of sequential machines used for manoeuvring output units (in our case the sequential machine for gate management);*
– *the third type of simple sequential machines consists of sequential machines to manage the two first types of sequential machines (these sequential machines will be assigned with the name of macro function sequential machines).*

In this case the procedure that the macro function sequential machine will perform will be as follows:

– idle state: *box powered by disconnectors;*
– commanded state: *execution by the operator of the gate*

apertura) e successivamente nello stato di bloccato.
Lo stato di bloccato della macchina sequenziale di macro funzione viene raggiunto automaticamente (in caso di corretto funzionamento delle apparecchiature) dallo stato di comandato.

– *stato di liberato*: comando di chiusura del cancello da parte dell'operatore. Il cancello viene sbloccato e successivamente manovrato in chiusura. Il controllo di chiusura porta la sua macchina sequenziale nello stato di liberato. Il controllo di chiusura del cancello attiva anche la liberazione del bloccamento dei sezionatori e il loro ritorno in posizione di chiusura. Il ritorno a riposo dei sezionatori interviene sulla macchina sequenziale di gestione del cancello riportandola nello stato di riposo.
– *stato di riposo*: lo stato di riposo, raggiunto dalla macchina sequenziale di gestione del cancello, fa transitare la macchina sequenziale di macro funzione dallo stato di liberato allo stato di riposo.

La macchina sequenziale di macro funzione può esser realizzata con due Flip Flop. Nel transito dallo stato "1" allo stato "2" e dallo stato "2" allo stato "3" di tale macchina sequenziale intervengono come ingressi gli stati delle macchine sequenziali dei vari sezionatori movimentati. Per il ritorno a riposo riceve lo stato di riposo della macchina sequenziale dell'organo d'uscita.

In fig. 8 viene rappresentata la macchina sequenziale complessa costituita da un insieme di macchine sequenziali più semplici, a due e a quattro stati, interagenti tra loro. Non sono state riportate tutte le relazioni esistenti tra le macchine al solo fine di render più leggibili le relazioni principali.

6. Gli apparati di sicurezza nell'ambito del segnalamento ferroviario

6.1. Premessa

Nel mondo ferroviario le macchine sequenziali in sicurezza hanno notevole importanza nella gestione dei movimenti dei veicoli ferroviari sia nell'ambito delle stazioni che in linea.

Le macchine sequenziali deputate alla movimentazione dei treni nelle stazioni, usualmente definite apparati centrali, nella loro evoluzione hanno realizzato progressive automatizzazioni diventando sempre più complesse.

Il cuore degli apparati centrali è costituito dalla formazione degli iti-

opening request command. This request will trigger the opening of all disconnectors involved in the box. A sequential safety machine type like the one seen in fig. 5 will manage each disconnector. The operator will receive an alert that the command was given correctly;

– locked state: *automatic return of opening and locking control of all disconnectors. Accumulation of the locking controls at opening of the disconnectors (AND of their controls) locks the macro function sequential machine and activates its output. The latter acts on the simple sequential machine that handles the opening of the gate (sequential machine in four states) that goes from standby state to controlled state (when opening) and later in the locked state.*
The locked state of the macro function sequential machine is reached automatically (in case of proper operation of equipment) from the commanded state.
– freed state: *gate closing command by the operator. The gate will be unlocked and then manoeuvred when closing. Closing control brings its sequential machine in the free state. The gate closing control also enables the release of blocking of disconnectors and their return to the closed position. The return to idle of the disconnec-*

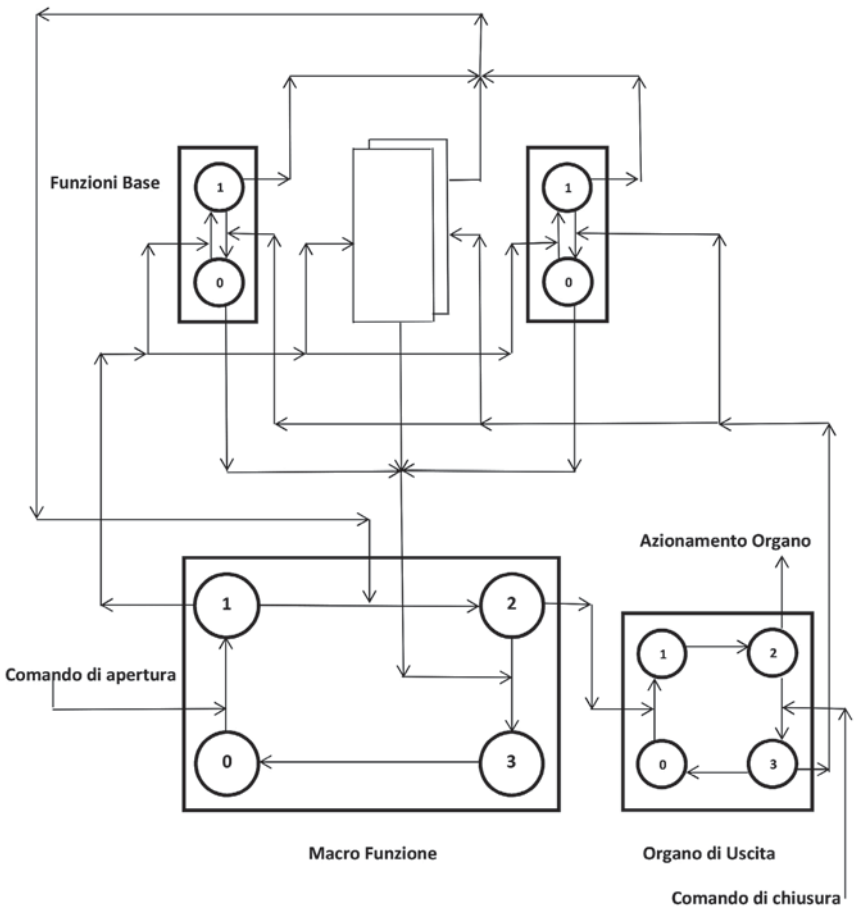

Fig. 8 - Schema di Macchina Sequenziale Complessa.
Fig. 8 - Diagram of complex sequential machine.

nerari che rappresentano i percorsi sicuri effettuabili dai treni all'interno delle stazioni.

Rispetto al primo apparato centrale elettrico a leve singole del 1924, dove per realizzare un itinerario l'operatore doveva movimentare diverse leve, oggi negli ACEI e negli ACC basta una pulsata (o una sequenza di pulsate) per predisporre il percorso del treno azionando deviatoi, PL e verificare la libertà della via.

Tra tutte le varietà di macchine sequenziali che hanno popolato gli impianti di segnalamento, prenderemo in esame quelle che gestiscono la formazione degli itinerari negli ACEI con liberazione elastica e le raffronteremo con le macchine sequenziali in sicurezza descritte nei punti precedenti.

Alla formazione degli itinerari provvede una macchina sequenziale in sicurezza complessa composta da più macchine sequenziali semplici. Queste sono costituite dalle macchine sequenziali deputate alla movimentazione dei deviatoi e dei PL e da una macchina sequenziale topografica che determina il percorso sicuro per il movimento del treno. Questa macchina sequenziale topografica è a sua volta costituita da due tipologie di macchine sequenziali tra loro interconnesse, una rappresentante la logica del punto origine, l'altra rappresentante la logica dei bloccamenti.

6.2. I deviatoi

Cominceremo con l'esaminare le macchine sequenziali dei deviatoi (quelle dei PL sono del tutto analoghe).

La Macchina sequenziale di un deviatoio è costituita da una macchina sequenziale asincrona a quattro stati realizzata con due relè combinatori.

Il relè combinatore è un dispositivo elettromeccanico dotato di due avvolgimenti elettrici. Può assumere due posizioni (stabili) a seconda di quale dei due avvolgimenti elettrici è stato attraversato per ultimo dalla corrente elettrica. La stabilizzazione della posizione è realizzata meccanicamente con una molla. L'ultimo avvolgimento percorso da corrente viene sezionato con un contatto di economia rappresentante lo stato del combinatore. Un relè combinatore rappresenta un bit di memoria come un singolo Flip Flop.

Il primo di questi due relè combinatori deputati alla gestione dei deviatoi è definito "combinatore di manovra" e viene indicato con M. Viene azionato dai comandi di itinerario che interessano il deviatoio richiedendolo posizionato normale o rovescio a seconda delle necessità.

Questo combinatore analizza la possibilità di manovra del deviatoio e ne rappresenta lo stato in cui lo vuole posizionato l'operatore (fig. 9).

Il secondo di questi due relè combinatori è definito "combinatore ausiliario" e viene indicato con A. Normalmente è in una posizione definita di "riposo", che impedisce l'alimentazione del deviatoio. Viene azionato dalla discordanza tra la posizione del deviatoio voluta dal combi-

tors intervenes on the sequential gate management machine taking it back to the idle state.

– idle state: *the idle state, reached by the sequential gate management machine makes the macro function sequential machine transit from the freed state to the idle state.*

The macro function sequential machine can be built with two Flip Flops. When transiting from state "1" to state "2" and from state "2" to state "3" of such sequential machine the states of the sequential machines of the different disconnectors act as inputs. For return to idle it receives the idle state of the sequential machine of the output unit.

Fig. 8 shows the complex sequential machine consisting of a set of simpler sequential machines, with two and four states, interacting with each other. All existing relations between the machines are not reported for readability of the main relations.

6. Security apparatus within railway signalling

6.1. Introduction

In the railway sector sequential safety machines have considerable importance in managing the movement of rail vehicles both in stations and online.

Sequential machines involved in the handling of trains at stations, usually defined central units, have made progressive automation in their evolution becoming increasingly complex.

The heart of central units consists of the formation of routes that represent the safe routes run by trains within the stations.

Compared to the first single lever electrical central units of 1924, where to make an itinerary the operator had to handle different levers, today in the ACEI and the ACC a pulse is sufficient (or a sequence of pulses) to prepare the train route by operating turnouts, rail crossing and ensure a clear track.

Among all the varieties of sequential machines that populated the signalling installations, we will examine those that manage the formation of routes in the ACEI with flexible clearing and we will compare them with the sequential safety machines described in the previous points.

The formation of routes is provided by a complex sequential safety machine composed of several sequential simple machines. These consist of sequential machines involved in the handling of turnouts and of rail crossing's and a topographical sequential machine determining the safe path for the movement of the train. This sequential topographical machine is in turn composed of two types of sequential interconnected machines, one representing the logic of the source point, the other representing the logic of blockings.

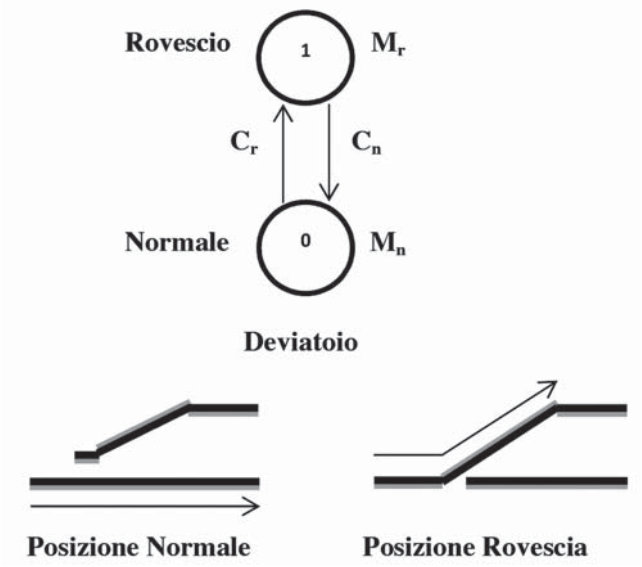

Fig. 9 - Macchina sequenziale del Combinatore M e rappresentazione delle direzioni percorribili.
Fig. 9 - Combiner M sequential machine and representation of accessible directions.

natore M e la posizione reale del deviatoio. Questa discordanza fa commutare il combinatore A nella posizione di "lavoro" abilitando l'alimentazione del deviatoio. La selezione di quale avvolgimento del motore del deviatoio sarà interessata dall'alimentazione abilitata dal combinatore A, è determinata dai contatti del combinatore M.

L'alimentazione al deviatoio permane sinché il deviatoio non raggiunge la posizione voluta dal combinatore M ripristinando la concordanza tra la posizione voluta dal combinatore M e la posizione reale del deviatoio. Ottenuta tale condizione il combinatore A ritorna nello stato di riposo togliendo l'alimentazione al deviatoio. La sua funzione corrisponde alla logica di gestione di un movimento controllata da un fine corsa (fig. 10).

L'azione integrata dei due combinatori realizza una macchina sequenziale a quattro stati rappresentante l'evoluzione del deviatoio sotto l'azione dei comandi di iti-

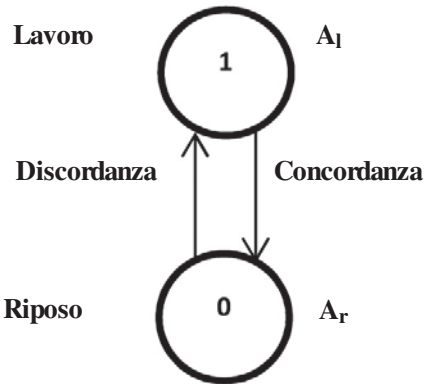

Fig. 10 - Macchina sequenziale del combinatore A.
Fig. 10 - Combiner A sequential machine.

6.2. Turnouts

We will start by examining the sequential turnout machines (rail crossing ones are quite similar). The sequential Machine of a turnout consists of a sequential asynchronous machine in four states made with two combiner relays.

The combiner relay is an electromechanical device with two electric windings. It has two positions (stable) depending on which of the two electric windings was the last to be crossed by electric current. The stabilisation of the position is mechanical with a spring. The last winding crossed by current is sectioned with an economic contact representing the combiner state. A combiner relay is a memory bit like a single Flip Flop.

The first of these two combiner relays for the management of turnouts is called "manoeuvre combiner," and is referred to by M. It is operated by route controls affecting the turnout requiring it to be positioned normal or reverse positioned according to needs.

This combiner analyses the manoeuvre possibility of the turnout and represents the state in which the operator wants it positioned (fig. 9).

The second of these two combiner relays is defined "auxiliary combiner" and is indicated with A. It is normally in a position defined "idle" that prevents feeding of the turnout. It is operated by the discrepancy between the position of the turnout desired by the M combiner and the actual position of the turnout. This discrepancy makes combiner A switch to the "work" position enabling power to the switch. The selection of which motor winding of the turnout will be affected in the event of power enabled by combiner A, is determined by the M combiner contacts.

Power to the switch remains until the turnout reaches the position desired by combiner M restoring the correlation between the position desired by combiner M and the actual position of the turnout. After obtaining that condition combiner A returns to the idle state cutting off power to the turnout. Its function corresponds to the management logic of a movement controlled by a limit switch (fig. 10).

The integrated action of the two combiners creates a sequential machine with four states representing the evolution of the turnout under the action of the route commands. Fig. 11 represents the states diagram where for the sake of simplicity the turnout position variation command and the discordance that appear between the position desired and the actual position is considered concurrent.

6.3. Topographic sequential machine

The topographic sequential machine [3] that produces, locks and clears the train route in a flexible way is one of the most efficient designs of sequential safety machines.

It consists of a sequential machine that manages the point where the train route starts inside the station and a

nerario. In fig. 11 viene rappresentato il diagramma a stati dove per semplicità si è considerato concomitante il comando di variazione di posizione del deviatoio e la discordanza che si viene a manifestare tra la sua posizione voluta e la posizione reale.

6.3. La macchina sequenziale topografica

La macchina sequenziale topografica [3] che realizza, blocca e libera in maniera elastica il percorso del treno è una delle progettazioni più efficienti di macchine sequenziali in sicurezza.

Essa è costituita da una macchina sequenziale che gestisce il punto in cui inizia il percorso del treno all'interno della stazione e da un insieme di macchine sequenziali che rappresentano alcuni degli elementi in cui è suddivisa la stazione (circuiti di binario - cdb) costituenti il percorso del treno.

Come esempio esplicativo della macchina sequenziale topografica, analizzeremo in fig. 12 un itinerario da percorrersi da parte di un treno in una stazione collocata su una linea a doppio binario e dotata di quattro binari di stazionamento (per semplicità di rappresentazione grafica in fig. 12 le comunicazioni sono state riassunte con il termine Dev).

Per un treno che entri in stazione dal punto 2 si possono predisporre quattro distinti itinerari in funzione del posizionamento delle comunicazioni. Indicheremo con Dev il posizionamento normale di una comunicazione e con Dev il posizionamento rovescio della stessa comunicazione. I quattro possibili itinerari uscenti dal Punto 2 saranno indicati con i punti di inizio e termine di percorso:

– 2 – I (Dev 1, Dev 2, Dev 4);
– 2 – II (Dev 1, Dev 2, Dev 4);
– 2 – III (Dev 1, Dev 2, Dev 3);
– 2 – IV (Dev 1, Dev 2, Dev 3).

Il posizionamento delle comunicazioni individua quali elementi (cdb) saranno interessati dal percorso del treno.

Sfruttando questa logica si può assemblare una macchina sequenziale complessa come quella di fig. 13 dove compaiono le macchine sequenziali semplici del punto

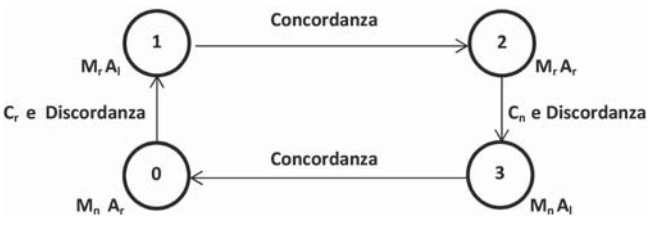

Fig. 11 - Macchina sequenziale complessiva del deviatoio.
Fig. 11 - Overall sequential machine of the turnout.

set of sequential machines that represent some of the elements in which the station is divided (track circuits) making up the train route.

As explanatory example of the topographic sequential machine, we will analyse a route in fig. 12 to be run by a train at a station on a double track line and with four stabling tracks (for simplicity of being represented graphically in fig. 12, the communications were summarised with the term Dev).

Four different routes can be arranged for a train entering the station from point 2 depending on the positioning of communications. We shall indicate with Dev the normal positioning of a communication and with Dev the reverse positioning of the same communication. The four possible routes exiting from Point 2 shall be indicated with the start and end points of the route:

– *2 – I → (Dev 1, Dev 2, Dev 4);*
– *2 – II → (Dev 1, Dev 2, Dev 4);*
– *2 – III → (Dev 1, Dev 2, Dev 3);*
– *2 – IV → (Dev 1, Dev 2, Dev 3).*

The placement of communications identifies which elements (track circuit) will be affected by the path of the train. Using this logic, a complex sequential machine can be assembled as that in fig. 13 where simple sequential machines of the source point (with four states) and path blockings (with two states) and their interactions appear.

– *R: itinerary registration relay. If excited it starts the supervision of the entities and the blocking of the route.*
– *V: route relay. If excited it confirms that the track circuits affecting the route are free.*
– *g_i: initial point connection relay. If de-energised it gives the go-ahead for blocking of the route.*
– *g_u: end point connection relay. If de-energised it attests blocking of the route.*
– *E: route control relay. If excited it attests both the blocking of the route and the control of the position desired by the entities involved in the itinerary.*

6.3.1. Source point sequential machine

The evolution of the source point sequential machine is described by two relays called R and Ap. For ease of description in the following steps we will attribute logical value "1" to the excited condition of the relay and logical value "0" to the de-energised condition of the relay. When idle, relay Ap, a stabilised relay, has logical value "1", while relay R, a neutral relay, has logical value "0". With the command of an itinerary originating at the point in question, after carrying out the necessary checks on the manoeuvrability of the turnouts and checking the absence of incompatibility, relay R switches to logical value "1" bringing the sequential machine in state "1". At this point the source point sequential machine awaits the implementation of the route

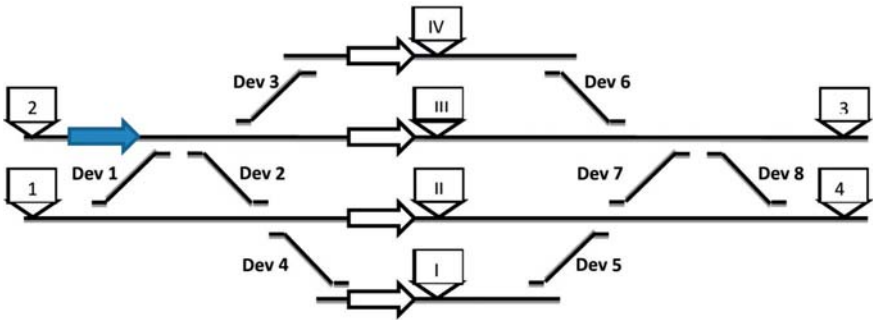

Fig. 12 - Punto origine e possibili percorsi per i treni.
Fig. 12 - Source point and possible train routes.

origine (a quattro stati) e dei bloccamenti del percorso (a due stati) e le loro interazioni.

- R: relè di registrazione itinerario. Se eccitato avvia il controllo degli enti e il bloccamento del percorso.
- V: relè di via. Se eccitato da conferma che i cdb interessanti l'itinerario sono liberi.
- g_i: relè di collegamento punto iniziale. Se diseccitato da il via al bloccamento del percorso.
- g_u: relè di collegamento punto finale. Se diseccitato attesta il bloccamento del percorso.
- E: relè di controllo del percorso. Se eccitato attesta sia il bloccamento del percorso che il controllo nella posizione voluta degli enti interessanti l'Itinerario.

6.3.1. La macchina sequenziale del punto origine

L'evoluzione della macchina sequenziale del punto origine è descritta da due relè denominati R ed Ap. Per semplicità di descrizione nei successivi passi attribuiremo alla condizione di eccitato del relè il valore logico "1" e alla

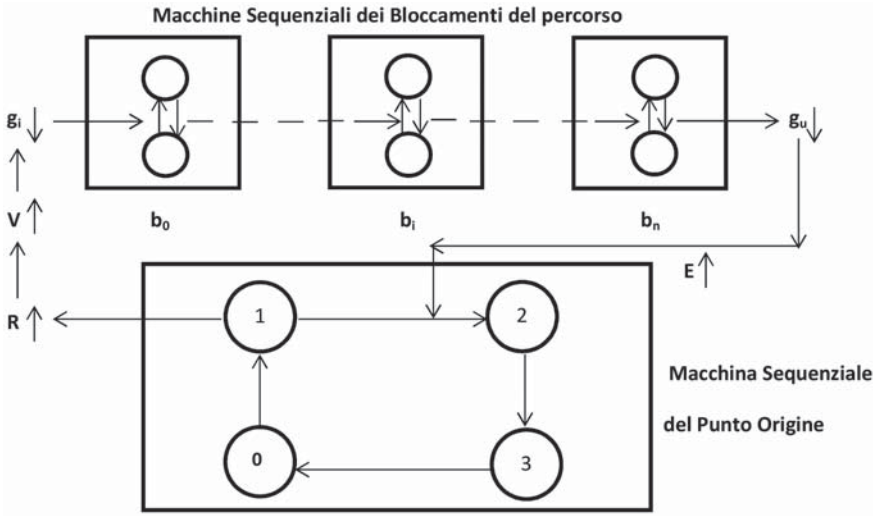

Fig. 13 - Macchina sequenziale complessa dell'itinerario.
Fig. 13 - Complex sequential machine of the itinerary.

blockings and the turnout position and rail crossing checks. Those conditions are summarised by logical value "1" of relay E that makes the sequential machine pass in state "2" with setting of the Ap relay to logical value "0". State "2" is the blocked state and activates the output that is able to give the green light signal. The movement of the train then manages the sequential machine. When the train passes the signal and occupies the permanent occupation track circuit, usually placed at 20 m (or slightly more) downstream of the signal, the sequential machine passes to state "3" identified by R to logic level "0". With the subsequent release of the track circuit permanent occupation, the sequential machine returns to state "0" with the setting of Ap relay to logical value "1". The source point sequential machine returns free and is available to complete another route. This is the first step of the flexible clearing followed by successive clearing of the other elements (track circuit) that constitute the route blocking. Fig. 14 shows the sequential machine of the source point.

The memory created by relay R compacts all possible outgoing route commands from the source point considered and any conditions of incompatibility for the route to be implemented. The physical implementation, after appropriate simplifications, is the classic one of the relay in stick[3] of which fig. 15 represents the states diagram and in fig. 16 the circuit implementation (single wire circuit) and the transition table.

The memory consisting of the magnetically stabilised Ap relay shows the time diagram in fig. 17.

The source point sequential machine is an asynchronous machine; for this reason, the transition from one state to the next should follow an encoding that results in the change of a single state variable (as in the Gray code[4]. This to avoid that which in technical terms is usually referred to as "path of state variables".

---

[3] The terminology "relay in stick" refers to a particular relay feeding circuit configuration. In this configuration a relay contact intervenes in parallel to other conditions provided for the feeding of the same relay thus shunting them as they fail.

[4] The Gray code is an (algebraically) weighted binary code. Its main property is as follows: the representation of any two consecutive natural numbers always consists of two strings of bits (of the same length) different from each other for the position of just one bit (Hamming distance equal to 1).

condizione di diseccitato del relè il valore logico “0”. A riposo il relè Ap, relè stabilizzato, risulta a valore logico “1”, mentre il relè R, relè neutro, risulta a valore logico “0”. Con il comando di un itinerario avente origine nel punto considerato, effettuate le opportune verifiche sulla manovrabilità dei deviatoi e verificata la non presenza di incompatibilità, il relè R passa al valore logico “1” portando la macchina sequenziale nello stato “1”. A questo punto la macchina sequenziale del punto origine rimane in attesa si attuino i bloccamenti del percorso e arrivino i controlli di posizione dei deviatoi e dei PL. Tali condizioni vengono riassunte dal valore logico “1” del relè E che fa transitare la macchina sequenziale nello stato “2” contraddistinto dal settaggio del relè Ap a valore logico “0”. Lo stato “2” costituisce lo stato di bloccato ed attiva l’uscita in grado di disporre a via libera il segnale. La macchina sequenziale viene di seguito gestita dal movimento del treno. Quando il treno supera il segnale ed occupa il Cdb di occupazione permanente, usualmente collocato a 20 m. (o poco più) a valle del segnale, la macchina sequenziale transita nello stato “3” contraddistinto da R a livello logico “0”. Con la successiva liberazione del Cdb di occupazione permanente la macchina sequenziale si riporta allo stato “0” con il settaggio del relè Ap a valore logico “1”. La macchina sequenziale del punto origine ritorna libera ed è disponibile per la realizzazione di altro itinerario. Questo è il primo passo della liberazione elastica cui seguirà la liberazione in successione degli altri elementi (cdb) che costituiscono il bloccamento del percorso. In fig. 14 viene riportata la macchina sequenziale del punto origine.

La memoria realizzata dal relè R compatta tutti i possibili comandi di itinerario uscenti dal punto origine considerato ed eventuali condizioni di incompatibilità per l’itinerario da realizzarsi. La realizzazione fisica, fatte le opportune semplificazioni, è quella classica del relè in stik[3] di cui in fig.15 viene rappresentato il diagramma a stati e in fig. 16 il circuito realizzativo (circuito unifilare) e la tabella di transizione.

La memoria costituita dal relè stabilizzato magneticamente Ap presenta il diagramma temporale di fig. 17.

La macchina sequenziale del punto origine è una macchina asincrona; per tal motivo il passaggio da uno stato al successivo deve seguire una codifica che comporti la modifica di una sola variabile di stato (come nel Codice Gray[4]). Ciò per evitare quella che nella terminologia tecnica viene usualmente definita “corsa delle variabili di stato”.

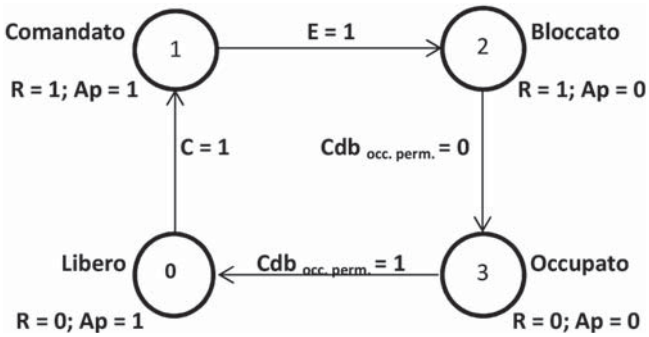

Fig. 14 - Macchina sequenziale punto origine.
Fig. 14 - Source point sequential machine.

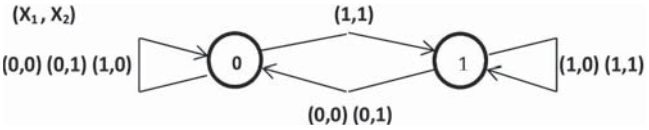

Fig. 15 - Diagramma a stati di un relè in stik.
Fig. 15 - State diagram of a relay in stik.

6.3.2. Route blocking sequential machines

The track circuits represent a topographical division of the Station signalling system. *Each Track circuit has two blocking cells depending on the direction of movement of the train. These blocking cells make up the* route blocking sequential machines.

These two sequential machines are two-state and embedded in each track circuit (one bit for each of the two machines); one variable is simply required, bd or bs depending on the direction of the route involving the track

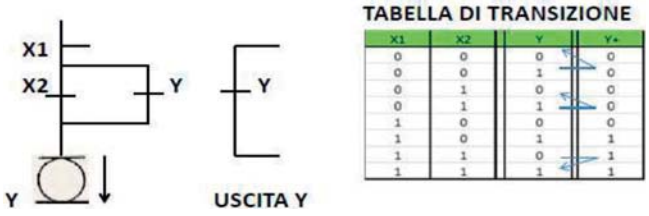

Fig. 16 - Circuito relè in stik e tabella di transizione.
Fig. 16 - Relay circuit in stik and transition table.

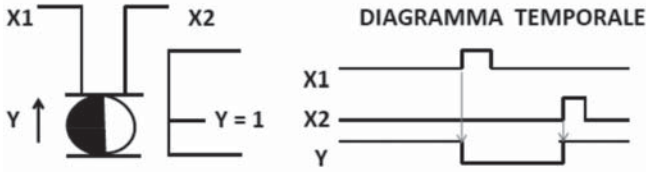

Fig. 17 - Diagramma temporale di relè stabilizzato magneticamente.
Fig. 17 - Time diagram of the magnetically stabilised relay.

---

(3) Con la terminologia “relè in stik” si intende una particolare configurazione circuitale di alimentazione di un relè. In tale configurazione un contatto del relè interviene in parallelo ad altre condizioni previste per l’alimentazione del relè stesso potendole così shuntare al loro venir meno.

(4) Il Codice Gray è un codice binario pesato (algebricamente). Sua principale proprietà è la seguente: la rappresentazione in codice Gray di due qualsiasi numeri naturali consecutivi è sempre costituita da due stringhe di bit (della stessa lunghezza) differenti tra loro per la posizione di un solo bit (distanza di Hamming uguale a 1).

6.3.2. Le macchine sequenziali dei bloccamenti di percorso

I cdb costituiscono una suddivisione topografica *dell'Impianto di Segnalamento di Stazione*. Ogni Cdb presenta due celle di bloccamento in dipendenza del senso di circolazione del treno. Tali celle di bloccamento costituiscono le *macchine sequenziali dei bloccamenti del percorso*.

Queste due macchine sequenziali incorporate in ogni Cdb sono a due stati (un bit per ognuna delle due macchine); sarà quindi sufficiente una sola variabile, bd o bs a seconda del senso dell'itinerario che interessa il cdb, per rappresentare l'evoluzione delle macchine sequenziali.

Tali macchine sequenziali sono realizzate con un relè in stik come si può vedere in fig. 18, dove è rappresentato il bloccamento per movimenti destri da parte del treno.

In tale macchina sequenziale sono presenti le seguenti variabili.

– bd_{ante} = Stato del bloccamento precedente rispetto la marcia del treno in grado di agire sul bd.
– Cbt = "OR" tra lo stato del Cdb ove insiste il bloccamento (libero = 1; occupato = 0) e una possibile manipolazione da parte dell'operatore.

La macchina sequenziale del bloccamento a riposo è nello stato di libero (stato "0") caratterizzato dalla variabile bd a livello logico "1".

Lo stato "1" di bloccato è raggiungibile con il transito di bd_{ante} a valore logico "0". (eccetto per il primo cdb da percorrere nel senso marcia treno per il quale non esiste un bd_{ante} ma una variabile gi) che porta il bd a livello logico "0".

Il ritorno allo stato "0" di libero si ha con l'AND logico di bd_{ante} a "1" e del Cdb, in cui è inserito il bd, a "1" (anche in questo caso eccetto il primo cdb senso marcia treno).

Da quanto sopra si evince che le macchine sequenziali dei bloccamenti del percorso propagano in cascata il passaggio della condizione da libero a bloccato (ogni bd_{ante} transitato nello stato di bloccato causa immediatamente il transito del bd successivo nello stato di bloccato); nel passaggio da bloccato a libero interviene anche la libertà del Cdb ove è inserito il bd (nella previsione logica del corretto funzionamento della macchina sequenziale tale transito deve avvenire dopo il passaggio del treno). Si ha quindi una progressiva e sequenziale commutazione dei bd verso lo stato di libero in conseguenza del transito del treno (fig. 19).

6.4. Riepilogo

La macchina sequenziale topografica dell'itinerario è alquanto simile allo schema di macchina sequenziale complessa rappresentata in fig. 8.

La logica del punto origine è assimilabile alla macchina sequenziale rappresentante la macro funzione, mentre le logiche dei bloccamenti di percorso sono assimilabili alle

circuit, to represent the evolution of sequential machines.

These sequential machines are made with a relay in stick as can be seen in fig. 18, where the blocking for right train movements are represented.

The following variables are included in such sequential machine.

– bd_{ante} *= Prior blocking state with respect to the train running capable of acting on the bd.*
– *Cbt = "OR" between the track circuit state where the blocking is (free = 1; busy = 0) and a possible manipulation by the operator.*

The sequential machine of the idle blocking is in a free state (state "0") characterised by variable bd at logical level "1".

Blocked state "1" can be reached with transit of bd_{ante} *with logical value "0" (except for the first track circuit to be run in the train direction for which there is no* bd_{ante} *but a variable gi) that brings the bd to logical level "0".*

Return to free state "0" occurs with logical AND of bd_{ante} *in "1" and the track circuit, where the bd is inserted, in "1" (in this case also except the first track circuit train direction).*

From the above it appears that route blocking sequential machines spread in cascade the condition from free to locked (every bd_{ante} *transited in the blocked state immediately causes the next bd transit in the blocked state); in the transit from blocked to free the freedom of Track circuit also intervenes where bd is inserted (in the logic prediction of correct operation of the sequential machine this transit must take after the transit of the train). Therefore there is a gradual and sequential switching of the bds to free state as a result of the transit of train (fig. 19).*

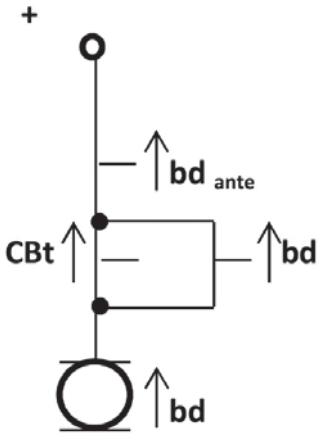

Fig. 18 - Circuito bd a relè.
Fig. 18 - Relay bd circuit.

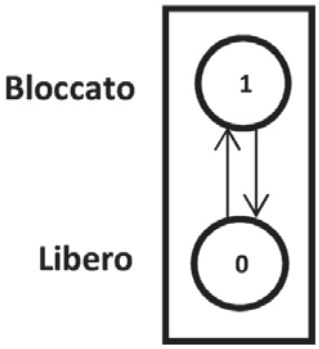

Fig. 19 - Macchina dei bloccamenti di percorso.
Fig. 19 - Route blocking machine.

funzioni base. La differenza fondamentale è rappresentata dal fatto che la macro funzione di fig. 8 controllava nel transito dallo stato "2" allo stato "3" il ritorno allo stato "0" di tutte le funzioni base, mentre nella macchina sequenziale topografica dell'itinerario lo stato di liberato (stato "3" nella macchina sequenziale del punto origine, stato "0" nei bloccamenti di percorso) viene attuato dall'avanzamento del treno. Questa modalità di liberazione progressiva, dapprima la macchina sequenziale del punto origine e poi in sequenza i bloccamenti di percorso, permette un'alta disponibilità della macchina sequenziale rendendo estremamente efficiente il sistema di gestione dei movimenti dei treni.

Di fatto l'itinerario bloccato in sicurezza per il movimento del treno si riduce progressivamente con l'avanzamento del treno stesso, rendendo disponibili gli elementi liberati (punto origine e Cdb già percorsi) per altri itinerari.

7. Analisi in termini di sicurezza della macchina sequenziale complessa dell'itinerario

Le macchine sequenziali in sicurezza presentano una loro affidabilità di funzionamento R(t). Per quanto possibile esse dovrebbero evitare che un guasto generico comporti una situazione di rischio. Anche per la macchina sequenziale degli itinerari si dovranno valutare gli eventi di guasto analizzando dove questi comportano non solo disservizio ma anche rischio per persone o cose. Ci limiteremo nella sottostante analisi ai soli guasti interessanti i relè costituenti le macchine sequenziali degli itinerari.

Prenderemo in esame le variabili C, E, $Cdb_{occ.\ perm.,}$ R ed Ap per la macchina sequenziale del punto origine e le variabili $bi_{ante,}$ CdB e bi per la macchina sequenziale del bloccamento del percorso (con il termine bi si intenderanno sia le variabili bd che le variabili bs a seconda del senso di circolazione del treno). Le considereremo quali variabili aleatorie e andremo a valutare l'effetto di un non voluto loro settaggio all'interno della macchina sequenziale semplice dove insistono.

Riassumiamo nella tabella 1 gli effetti di un settaggio errato.

- Definiremo P1up(E) la probabilità di errore di un relè neutro eccitato (ossia si disecciti per guasto);
- definiremo P1dw(E) la probabilità di errore di un relè neutro diseccitato (ossia si ecciti per guasto);
- definiremo P2up(E) la probabilità di errore di un relè stabilizzato eccitato (ossia si disecciti per guasto);
- definiremo P2dw(E) la probabilità di errore di un relè stabilizzato diseccitato (ossia si ecciti per guasto).

Gli eventi, causa di errato settaggio dei relè neutri, sono principalmente le alimentazioni e le disalimentazioni indebite. Attribuiremo agli eventi costituiti dalle disalimentazioni indebite una probabilità di accadimento maggiore rispetto agli eventi costituiti dalle alimentazioni indebite. Tale diversa probabilità comporterà P1up(E) >

6.4. Summary

The topographic sequential machine is rather similar to the complex sequential machine shown in fig. 8.

The logic of the source point can be assimilated to the sequential machine representing the macro function, while the route blocking logics can be assimilated to the base functions. The main difference is represented by the fact that the macro function in fig. 8 controlled in the transit the return to state "0" of all base functions from state "2" to state "3", while in the topographic sequential machine of the itinerary the freed state (state "3" in the source point sequential machine, state "0" in the route blockings) is implemented by the train movement. This gradual release method, initially the sequential machine of the source point and then the route blocking in sequence, allows great availability of the sequential machine making the train movement management system extremely efficient.

In fact, the safely blocked itinerary for the movement of trains gradually decreases as the same train progresses, making the released elements available (source point and track circuit already run) for other itineraries.

7. Analysis in terms of safety of the route complex sequential machine

Sequential safety machines have their own operating reliability R(t). As much as possible they should prevent that a generic failure results in a hazardous situation. Even for route sequential machines failure events should be analysed where these involve not only disruption but also risk to persons or property. We will just deal with faults involving relays constituting itinerary sequential machines in this analysis.

We will examine the variables C, E, track $circuit_{occ.\ perm.,}$ *R and Ap for the source point sequential machine and variables* $bi_{ante,}$ *Track circuit e bi for the route blocking sequential machine (the term bi is to be understood both as the variables bd and the variables bs depending on the direction of movement of the train). We will consider them as random variables and will evaluate the effect of their unwanted setting within the simple sequential machine they stand on.*

The effects of incorrect setting are summarised in table 1.

- *We shall define P1up(E) the probability of failure of an energised neutral relay (i.e. it de-energises due to failure);*
- *we shall define P1dw(E) the probability of failure of a de-energised neutral relay (i.e. it energises due to failure);*
- *we shall define P2up(E) the probability of failure of an*

TABELLA 1 – *TABLE 1*

Macchina sequenziale del punto origine
Source point sequential machine

Stato attuale ***Current state***	**Settaggio variabile** ***Variable setting***	**Stato futuro** ***Future state***	**Note** ***Notes***
Variabile C - *Variable C*			
Stato 0 *State 0*	C ↑	Stato 1 *State 1*	Se tutti i deviatoi interessati da C sono liberi bloccherà l'itinerario *If all turnouts affected by C are free it will block the route*
Stato 1 *State 1*	C ↓	Stato 0 *State 0*	Distrugge l'itinerario registrato *It destroys the recorded route*
Stato 2 *State 2*	C ↓	Stato 3 *State 3*	C ↓ → R ↓. Dispone il segnale a via impedita prima dell'occupazione *C ↓ → R ↓. It puts signal at danger before occupation*
Stato 3 *State 3*	C ↑	Stato 3 *State 3*	Quando $Cdb_{occ.perm.}$ ↑ → R ↑ si registra di nuovo l'itinerario *When Track circuit$_{occ.perm.}$ ↑ → R ↑ the new itinerary is recorded*
Variabile E – *Variable E*			
Stato 0 *State 0*	E ↑	Stato 3 *State 3*	Ap ↓ → R ↓ *Ap ↓ → R ↓*
Stato 1 *State 1*	E ↑	Stato 2 *State 2*	Dispone a via libera il segnale prima dell'acquisizione controllo enti *It puts the green light signal before acquisition of control of entities*
Stato 2 *State 2*	E ↓	Stato 2 *State 2*	Resta Ap ↓. Segnale a via impedita prima dell'occupazione *Ap ↓ remains. Signal at danger before occupation*
Stato 3 *State 3*	E ↑	Stato 3 *State 3*	Resta Ap ↓ quando $Cdb_{occ.perm.}$ ↑ *Ap ↓ remains when Track circuit$_{occ.perm.}$ ↑*
Variabile $Cdb_{occ.perm.}$ - *Variable Track circuit$_{occ.perm.}$*			
Stato 0 *State 0*	$Cdb_{occ.perm.}$ ↓	Stato 0 *State 0*	Resta Ap ↑ *Ap ↑ remains*
Stato 1 *State 1*	$Cdb_{occ.perm}$ ↓	Stato 0 *State 0*	Comporta (dopo sequenza) **R** ↓ → E ↓ → Ap ↑ *It involves (after sequence) **R** ↓ → E ↓ → Ap ↑*
Stato 2 *State 2*	$Cdb_{occ.perm}$ ↓	Stato 3 *State 3*	Comporta R ↓. Segnale a via impedita prima dell'occupazione *It involves R ↓. Signal at danger before occupation*
Stato 3 *State 3*	$Cdb_{occ.perm.}$ ↑	Stato 0 *State 0*	Anticipo della liberazione del punto origine *Advance clearing of source point*
Variabile R – *Variable R*			
Stato 0 *State 0*	R ↑	Stato 1	In base allo stato dei deviatoi si realizzerà un itinerario *Depending on the state of the turnouts a route will be created*
Stato 1 *State 1*	R ↓	Stato 0 *State 0*	Distrugge l'itinerario registrato *It destroys the recorded route*
Stato 2 *State 2*	R ↓	Stato 3 *State 3*	Dispone il segnale a via impedita prima dell'occupazione *It puts signal at danger before occupation*
Stato 3 *State 3*	R ↑	Stato 2 *State 2*	Quando $Cdb_{occ.perm.}$ ↑ si registra di nuovo l'itinerario *When Track circuit$_{occ.perm.}$ ↑ the route is recorded again*
Variabile Ap - *Variable Ap*			
Stato 0 *State 0*	Ap ↓	Stato 3 *State 3*	La macchina si blocca in quanto Ap ↓ → R ↓ *The machines is blocked as Ap ↓ → R ↓*
Stato 1 *State 1*	Ap ↓	Stato 2 *State 2*	Quando E ↑, si disposizione a via libera il segnale *When E ↑, green light is available*
Stato 2 *State 2*	Ap ↑	Stato 1 *State 1*	Disposizione a via impedita del segnale *Signal at danger is available*
Stato 3 *State 3*	Ap ↑	Stato 0 *State 0*	Anticipa il ritorno a riposo della macchina sequenziale *Return to idle of the sequential machine is anticipated*

(continua)
(to be continued)

(segue) TABELLA 1 – *TABLE 1*

Macchina sequenziale del punto origine
Source point sequential machine

Stato attuale ***Current state***	**Settaggio variabile** ***Variable setting***	**Stato futuro** ***Future state***	**Note** ***Notes***
Macchina sequenziale del bloccamento ***Blocking sequential machine***			
Variabile bi_{ante} - *Variable* bi_{ante}			
Stato 0 *State 0*	bi_{ante} ↓	Stato 1 *State 1*	Blocca l'ente *It blocks the entity*
Stato 1 *State 1*	bi_{ante} ↑	Stato 0 *State 0* Stato 1 *State 1*	Se Cdb ↑ → libera l'ente *If Track circuit* ↑ → *entity is cleared* Se Cdb ↓ → l'ente rimane bloccato *If Track circuit* ↓ → *the entity remains blocked*
Variabile Cdb - *Variable Track circuit*			
Stato 0 *State 0*	Cdb ↓	Stato 0 *State 0*	Non causa bloccamento dell'ente *It does not cause blocking of the entity*
Stato 1 *State 1*	Cdb ↑	Stato 0 *State 0* Stato 1 *State 1*	Se bi_{ante} ↑ → libera l'ente *If* bi_{ante} ↑ → *entity is cleared* Se bi_{ante} ↓ → l'ente rimane bloccato *If* bi_{ante} ↓ → *the entity remains blocked*
Variabile bi - *Variable bi*			
Stato 0 *State 0*	bi ↓	Stato 1 *State 1*	Blocca l'ente *It blocks the entity*
Stato 1 *State 1*	bi ↑	Stato 0 *State 0*	Libera l'ente *Entity is cleared*

P1dw(E). Gli eventi causa di errato settaggio dei relè stabilizzati sono principalmente le alimentazioni indebite, le interferenze magnetiche e le possibili smagnetizzazioni del magnete permanente dei relè. Ritenendo equiprobabili le alimentazioni indebite alla bobina di eccitazione o alla bobina di diseccitazione del relè stabilizzato come pure le interferenze magnetiche nei confronti del magnete permanente, resta diseguale nella probabilità degli eventi causati dalla smagnetizzazione del magnete permanente. In quest'ultimo caso il relè stabilizzato assumerebbe un comportamento da relè neutro manifestando sensibilità anche alle disalimentazioni. Ne consegue che risulterà anche in questo caso P2up(E) > P2dw(E).

Ragionevolmente si può ritenere P1up(E) > P2up(E) > P2dw(E) > P1dw(E).

Prendendo in esame la tabella 1, si evidenziano quattro possibili rischi che di seguito vengono elencati:

– disposizione a via impedita del segnale prima del transito del treno (con macchina sequenziale del punto origine nello Stato 2 a seguito di diseccitazione indebita di C, R, E o $Cdb_{occ.\ perm.}$ o di eccitazione indebita di Ap);
– disposizione a via libera del segnale prima dell'acquisizione del controllo e del bloccaggio degli enti (con macchina sequenziale del punto origine nello stato 1 a seguito di eccitazione indebita di E);
– formazione Itinerari non voluti (con macchina se-

energised stabilised relay (i.e. it de-energises due to failure);

– *we shall define P2dw(E) the probability of failure of a de-energised stabilised relay (i.e it energises due to failure).*

The events, due to incorrect setting of neutral relays, are mainly feeds and undue power failures. We shall attribute the events constituted by undue power failures with a greater probability of occurrence than events constituted by undue powers. Such different probability will result in P1up(E) > P1dw(E). The events due to incorrect setting of stabilised relays are mainly undue powers, magnetic interferences, and possible demagnetising of permanent magnet relays. Considering undue powers at the excitation coil or de-energising coil of the stabilised relay as well as magnetic interferences against the permanent magnet, it remains uneven in the probability of events caused by demagnetisation of the permanent magnet. In the latter case the stabilised relay would assume a neutral relay behaviour manifesting sensitivity also at power failures. It follows that P2up (E) > P2dw (E).

Reasonably P1up(E) > P2up(E) > P2dw(E) > P1dw(E) can be considered.

Examining table 1, there are four possible risks that are listed below:

– *signal at danger available before the train transit (with*

quenziale del punto origine nello stato 0 a seguito di eccitazione indebita di C o R; con la macchina sequenziale del punto origine nello stato 3 a seguito di eccitazione indebita di C o R);

– liberazione anticipata dell'itinerario con treno in percorso (con la macchina sequenziale del bloccamento nello stato 1 a seguito di bi eccitato indebitamente o bi_{ante} eccitato indebitamente con Cdb eccitato o Cdb eccitato indebitamente con bi_{ante} eccitato).

I quattro possibili rischi sono quasi tutti dovuti ai soli guasti dei relè neutri.

Attribuiremo ai quattro eventi sopra identificati dei livelli di pericolosità crescenti per i danni che possono causare qualora avessero a verificarsi i rischi evidenziati.

Evento 1, E1: disposizione a via impedita del segnale prima del transito del treno (una brusca frenata del treno potrebbe causare danni ai passeggeri); *peso pericolosità:* $p_1 = 10^{-1}$;

Evento 2, E2: formazione indebita di itinerari (l'itinerario non voluto potrebbe interessare un binario interrotto ove operano persone con loro investimento); *peso pericolosità:* $p_2 = 10^2$;

Evento 3, E3: disposizione a via libera del segnale prima dell'acquisizione del controllo e del bloccaggio degli enti (il controllo di un ente potrebbe non pervenire – ulteriore guasto – mettendo a rischio la marcia del treno - possibile deragliamento); *peso pericolosità:* $p_3 = 10^3$;

Evento 4, E4: liberazione anticipata dell'itinerario (la liberazione anticipata degli enti potrebbe permettere il loro riutilizzo creando situazioni di estremo pericolo – possibile investimento di automezzi se presenti PL o scontro tra treni); *peso pericolosità:* $p_4 = 10^5$.

Ipotizzeremo poi delle probabilità di rischio per tali eventi qualora P1up(E) = P1dw(E) = P2dw = 1 (ossia abbiano a verificarsi guasti ai soli relè della macchina sequenziale).

– $Pr(E1) = 10^{-1}$ (considereremo che quasi sempre la disposizione a via impedita del segnale prima del transito del treno causi una brusca frenata e che ciò possa causare qualche inconveniente ai passeggeri);
– $Pr(E2) = 10^{-5}$ (considereremo estremamente improbabile che si possa realizzare un itinerario su un binario interrotto e che il personale eventualmente al lavoro sia investito dal treno);
– $Pr(E3) = 10^{-4}$ (considereremo improbabile che si manifesti un altro guasto quale il mancato controllo di un deviatoio incontrato di punta dal treno e che ciò possa causare uno svio con conseguenze gravi);
– $Pr(E4) = 10^{-5}$ (considereremo estremamente improbabile che il tempo intercorso tra la liberazione degli enti e il loro riutilizzo comporti uno scontro tra treni o un investimento con mezzi stradali su PL eventualmente presenti sugli itinerari).

Valutiamo ora la probabilità si manifestino gli eventi

sequential machine of the source point at State 2 point following undue de-energising of C, R, E, or Track circuit$_{occ\ perm.}$ or undue energising of Ap);

– *green light signal available before the acquisition of control and of blocking of entities (with sequential machine of the source point in state 1 as a result of undue energising of E);*
– *formation of unwanted Routes (with sequential machine of source point in state 0 as a result of undue energising of C or R; with sequential machine of the source point at state 3 as a result of undue de-energising of C or R);*
– *early clearing of route with train on route (with the blocking sequential machine in State 1 as a result of bi unduly energised or bi_{ante} unduly energised with Track circuit energised or Track circuit unduly energised with bi_{ante} energised).*

The four possible risks are almost all due to neutral relay failures.

We shall attribute increasing levels of hazard to the four events identified above for any damage that they may cause should the risks highlighted occur.

Event 1, E1: signal at danger available before the train transit (sharp braking of the train could cause damage to passengers); *hazard weight* $p_1 = 10^{-1}$;

Event 2, E2: undue formation of routes (unwanted route could affect an interrupted track where people work and their running over); *hazard weight:* $p_2 = 10^2$;

Event 3, E3: green light signal available before the acquisition of control and blocking of entities (the control of an entity may not be received – further failure – risking train operation – possible derailment); *hazard weight:* $p_3 = 10^3$;

Event 4, E4: early clearing of route (the early clearing of entities may allow their reuse by creating extremely dangerous situations – possible hitting of if rail crossings are present or crash between trains); *hazard weight:* $p_4 = 10^5$.

We will assume the likelihood of risk for such events if P1up(E) = P1dw(E) = P2dw = 1 (i.e. only sequential machine relays failures occur.

– $Pr(E1) = 10^{-1}$ *(we will consider that almost always signal at danger available before the train transit causes sharp braking and that this may cause some inconvenience to passengers);*
– $Pr(E2) = 10^{-5}$ *(we will consider extremely unlikely that an itinerary is created on an interrupted track and that staff possibly at work is run over by the train);*
– $Pr(E3) = 10^{-4}$ *(we will consider unlikely that another failure occurs such as failure to monitor a turnout found at the head of the train and that this will cause a deviation with serious consequences);*

E1, E2, E3 ed E4 facendo riferimento solamente ai guasti dei relè presenti nelle macchine sequenziali degli itinerari.

Le popolazioni di variabili aleatorie presenti nelle macchine sequenziali degli itinerari di un apparato di sicurezza non sono tra loro uguali. Nella totalità delle macchine sequenziali dei punti origine presenti in un apparato di sicurezza si hanno le seguenti relazioni tra le varie popolazioni di variabili aleatorie considerate:

$$(Cdb_{occ.perm.} = E = R = Ap) < C$$

nella totalità delle macchine sequenziali dei bloccamenti presenti in un apparato di sicurezza si hanno le seguenti relazioni tra le popolazioni delle variabili aleatorie considerate:

$$(bi \sim bi_{ante}) = 2\ Cdb$$

In un impianto similare a quello rappresentato in fig. 12 possiamo ipotizzare la presenza delle seguenti popolazioni di variabili aleatorie:

$$bi = bi_{ante} = 40; \quad C = 32; \quad E = R = Ap = Cdb_{occ.perm.} = 12$$

Inoltre, se si ritengono i guasti dei relè uniformemente distribuiti nel tempo, si dovranno valutare percentualmente i tempi di permanenza delle macchine sequenziali nei vari stati. Ipotizzeremo che nelle macchine sequenziali del punto origine il rapporto tra il tempo di permanenza nello stato 0 e il tempo di permanenza nello stato 2 sia pari a 10; così pure sia di valore 10 il rapporto tra il tempo di permanenza nello Stato 2 e il tempo di permanenza negli Stati 1 e 3. Per le macchine sequenziali dei bloccamenti ipotizzeremo che il rapporto tra il tempo di permanenza nello stato 0 e il tempo di permanenza nello Stato 1 sia ancora di valore 10. I tempi di permanenza negli stati 0 delle macchine sequenziali dei punti origine e negli stati 0 delle macchine sequenziali dei bloccamenti si possono ragionevolmente ritenere uguali commettendo un errore non significativo per la presente trattazione. Analogamente, per i bassi valori di P1up, P1dw e P2dw, si possono ritenere trascurabili le probabilità congiunte di due o più eventi di guasto rispetto alla probabilità di un singolo guasto.

Con queste semplificazioni si possono calcolare le probabilità di accadimento di eventi che possono sfociare in rischi a seguito di avarie dei relè costituenti le macchine sequenziali:

$$P(E) = \Sigma\ (N_{Pi} \cdot {}^{Tsi}/_{T} \cdot P1up + N_{pi} \cdot {}^{Tsi}/_{T} \cdot P1dw + N_{pi} \cdot {}^{Tsi}/_{T} \cdot P2dw)$$

Nell'equazione del calcolo di P(E)

- N_{Pi} sono le popolazioni di variabili aleatorie che concorrono al verificarsi di P(E);
- ${}^{Tsi}/_{T}$ rappresenta il rapporto tra il tempo di permanenza nello stato della macchina sequenziale in cui si verifica P(E) e il tempo totale di evoluzione.

Sempre nel caso di un impianto come quello di fig. 12 si ottengono i seguenti valori di probabilità di accadimento per i quattro eventi considerati:

- $P(E1) = 6{,}1 \cdot P1up + 1\ P2dw$;
- $P(E2) = 40 \cdot P1dw$;
- $Pr(E4) = 10^{-5}$ *(we will consider extremely unlikely that the time elapsed between the clearing of entities and their reuse involves a crash between trains or running over with road transport on rail crossings if any on the routes).*

Let us now evaluate the probability of events E1, E2, E3 and E4 referring only to faults of relays on sequential machines of routes.

The populations of random variables in route sequential machines of a safety apparatus are not equal. In the totality of sequential machines of source points in a safety apparatus we have the following relationships between the various populations of random variables considered:

$$(Track\ circuit_{occ.perm.} = E = R = Ap) < C$$

in the totality of blocking sequential machines in a safety apparatus we have the following relationships between the populations of random variables considered:

$$(bi \sim bi_{ante}) = 2\ Track\ circuit$$

In a system similar to the one shown in fig. 12 we can assume the following populations of random variables:

$$bi = bi_{ante} = 40; \quad C = 32; \quad E = R = Ap = Track\ circuit_{occ.perm.} = 12$$

Also, if the relay failures are believed to be uniformly distributed over time, the percentage stay time of sequential machines in various States must be evaluated. We will assume that the source point sequential machines relationship between stay time in state 0 and the stay time in state 2 is 10; and also that the ratio between stay time in State 2 and stay time in State e and 3 is 10. For blocking sequential machines we will assume that the ratio between stay time in state 0 and stay time in State 1 is still 10. Stay times of the source point sequential machines in state 0 and of the blocking sequential machines in state 0 can be reasonably considered the same making a negligible mistake for this dissertation. Similarly, for low value of P1up, P1dw and P2dw the joint probabilities of two or more events of failure with respect to the likelihood of a single failure must be considered negligible.

With these simplifications the probability of occurrence of events that may lead to risks as a result of failures of sequential machines constituent relays can be calculated:

$$P(E) = \Sigma\ (N_{Pi} \cdot {}^{Tsi}/_{T} \cdot P1up + N_{pi} \cdot {}^{Tsi}/_{T} \cdot P1dw + N_{pi} \cdot {}^{Tsi}/_{T} \cdot P2dw)$$

In the equation of calculating P(E)

- N_{Pi} *are populations of random variables that contribute to the occurrence of P(E);*
- ${}^{Tsi}/_{T}$ *represents the ratio of the length of stay in the state of the sequential Machine where P(E) occurs and the total time of evolution.*

In addition, in the case of a system like the one shown in fig. 12 the following values of probability of occurrence for the four events considered are obtained:

- $P(E1) = 6{,}1 \cdot P1up + 1\ P2dw$;

– P(E3) = 0,1 · P1dw;

– P(E4) = 3,6 · P1dw.

Qualora poi si presuppongano le seguenti relazioni:

– P1up = 10 · P1dw e P2dw = 3 · P1dw;

si possono esprimere le P(E) in funzione di P1dw ottenendo le sottostanti relazioni:

– P(E1) = 64 · P1dw;

– P(E2) = 40 · P1dw;

– P(E3) = 0,1 · P1dw;

– P(E4) = 3,6 · P1dw.

Ritenendo indipendenti gli eventi legati alle P1dw, P1up e P2dw con gli eventi legati alle Pr(E), si possono ottenere le probabilità di accadimento di rischio legate ai guasti dei relè delle Macchine sequenziali degli Itinerari:

– $Pr(E1) \cdot P(E1) = 64 \cdot 10^{-1} \cdot P1dw$;

– $Pr(E2) \cdot P(E2) = 40 \cdot 10^{-5} \cdot P1dw$;

– $Pr(E3) \cdot P(E3) = 0,1 \cdot 10^{-4} \cdot P1dw$;

– $Pr(E4) \cdot P(E4) = 3,6 \cdot 10^{-5} \cdot P1dw$.

Associando a tali Probabilità i pesi delle pericolosità legati agli eventi si ottengono i seguenti livelli di rischio LR:

– $LR1 = p_1 \cdot Pr(E1) \cdot P(E1) = 0,64 \cdot P1dw$;

– $LR2 = p_2 \cdot Pr(E2) \cdot P(E2) = 0,04 \cdot P1dw$;

– $LR3 = p_3 \cdot Pr(E3) \cdot P(E3) = 0,01 \cdot P1dw$;

– $LR4 = p_4 \cdot Pr(E4) \cdot P(E4) = 3,6 \cdot P1dw$.

La situazione più pericolosa (per il solo guasto dei relè presenti nelle macchine sequenziali degli itinerari con i dati ipotizzati) è rappresentata della liberazione anticipata dell'itinerario. Tale situazione pericolosa probabilmente risulterebbe ancor più accentuata se si prendessero in considerazione gli altri eventi che intervengono nella formazione e utilizzo degli itinerari (basta pensare alla mancata occupazione da parte del treno di un Cdb).

Il motivo principale di tale pericolosità è insito nella struttura con cui è realizzata la macchina sequenziale dei bloccamenti. Con due soli stati (un bit) essa rappresenta quanto di più efficiente si possa realizzare; nel contempo con due soli stati essa non permette un'architettura protetta nei confronti di guasti evitando che questi abbiano ad influenzare la sicurezza del sistema (come potrebbe invece farsi con una macchina a quattro stati).

8. Conclusioni

Le macchine sequenziali in Sicurezza rappresentano un importante sottoinsieme degli automi; esse realizzano procedure che impediscono errori nell'esecuzione sequenziale di comandi a cura degli operatori.

Nella loro evoluzione ciclica le macchine sequenziali in sicurezza presentano stati che vengono definiti con il termine di "bloccato"; tali stati contraddistinguono i mo-

– *P(E2) = 40 · P1dw;*

– *P(E3) = 0,1 · P1dw;*

– *P(E4) = 3,6 · P1dw.*

Should the following ratios be assumed:

– *P1up = 10 · P1dw e P2dw = 3 · P1dw;*

P(E) can be expressed as a function of P1dw obtaining the ratios below:

– *P(E1) = 64 · P1dw;*

– *P(E2) = 40 · P1dw;*

– *P(E3) = 0,1 · P1dw;*

– *P(E4) = 3,6 · P1dw.*

Considering the events related to P1dw, P1up and P2dw independent with events related to Pr(E), the probability of occurrence of risks related to faults of route sequential machines relays can be obtained:

– $Pr(E1) \cdot P(E1) = 64 \cdot 10^{-1} \cdot P1dw$;

– $Pr(E2) \cdot P(E2) = 40 \cdot 10^{-5} \cdot P1dw$;

– $Pr(E3) \cdot P(E3) = 0,1 \cdot 10^{-4} \cdot P1dw$;

– $Pr(E4) \cdot P(E4) = 3,6 \cdot 10^{-5} \cdot P1dw$.

By associating the weight hazards related to the events to these Probabilities, the following LR risk levels are obtained:

– $LR1 = p_1 \cdot Pr(E1) \cdot P(E1) = 0.64 \cdot P1dw$;

– $LR2 = p_2 \cdot Pr(E2) \cdot P(E2) = 0.04 \cdot P1dw$;

– $LR3 = p_3 \cdot Pr(E3) \cdot P(E3) = 0.01 \cdot P1dw$;

– $LR4 = p_4 \cdot Pr(E4) \cdot P(E4) = 3.6 \cdot P1dw$.

The most dangerous situation (only for the failure of the relays on the route sequential machines with data assumed) is represented in the early clearing of the itinerary. This dangerous situation would probably be even more pronounced if other events involved in the formation and use of the routes were to be considered (just think of the lack of occupation of a track circuit by the train).

The main reason for such danger is inherent in the structure with which the blocking sequential machine is built. With only two states (one bit) it represents the most efficient that can be achieved; at the same time with only two states it does not allow an architecture protected against failures while avoiding them to affect the safety of the system (as could be done with a four state machine).

8. Conclusions

Sequential safety machines are an important subset of automata; they perform procedures that prevent errors in sequential execution of commands by the operators.

In their cyclic evolution sequential safety machines have states that have been defined with the term "blocked";

menti in cui si effettuano operazioni pericolose per persone o cose e pertanto la macchina si assume il compito di eseguire la corretta sequenza di operazioni per evitare danni alle stesse.

Le macchine sequenziali in sicurezza hanno interessato l'automatizzazione del mondo industriale intervenendo in molti settori, dalla gestione automatica di fonderie agli interventi manutentivi su apparecchiature elettriche disalimentate.

In particolare, però, è stato nel segnalamento ferroviario che hanno prodotto sistemi di notevole complessità atti a definire una vera e propria disciplina della sicurezza.

Le procedure di sicurezza attuate degli apparati di segnalamento sono state nel tempo realizzate con automatismi implementanti tecnologie diverse; si è comunque sempre mantenuta la filosofia di base riguardante i collegamenti di sicurezza da realizzarsi tra i dispositivi d'impianto e i segnali.

Uno degli aspetti più critici nella gestione degli apparati di segnalamento è costituito dalle necessarie modifiche da introdurvisi in conseguenza di modifiche apportate ai piani del ferro di un impianto. Tali modifiche, interessando macchine sequenziali complesse, sono laboriose e complicate. Uno studio che possa segregare le varie macchine sequenziali complesse in macchine sequenziali più semplici potrebbe essere di aiuto nell'identificazione di quali relazioni tra le macchine sono da modificarsi, agevolando il lavoro di progettisti e tecnici manutentori.

these states represent the times when hazardous operations are performed for people or property and therefore the machine assumes the task of performing the correct sequence of operations to prevent damage to the same.

Sequential safety machines have affected the automation industry by intervening in many sectors, from the automatic management of foundries to maintenance operations on electrical appliances not powered.

In particular, however, it was in the railway signalling that they produced remarkably complex systems suitable to define a real discipline of safety.

Safety procedures implemented by signalling equipment were made over time with automated technologies implementing different technologies; the basic philosophy regarding safety connections to be made between devices and signals has however been maintained.

One of the most critical aspects of signalling equipment management consists of the necessary amendments to be introduced as a result of changes to the rail level of a system. Those changes, affecting complex sequential machines are laborious and complicated. A study that would segregate the various complex sequential machines in simpler machines could be helpful in identifying what relationships are to be changed between the machines, facilitating the work of designers and maintenance technicians.

BIBLIOGRAFIA - *REFERENCES*

[1] W. Ross Ashby, *"Introduzione alla Cibernetica",* Einaudi 1971.

[2] Giacomo Cioffi, *"Lezioni di Sistemi Combinatori e Sequenziali",* Ed. Siderea 1974.

[3] Gabriele Pupolin, *"Descrizione della macchina sequenziale degli itinerari negli ACEI",* in La Tecnica Professionale, novembre 2014.