Common Information Factor Analysis and Its Application on Railway Signalling System

Xiaoli She

Engineer, Beijing National Railway Research & Design Institute of Signal & Communication Co., Ltd.

Guoliang Gao

Senior Engineer, Beijing National Railway Research & Design Institute of Signal & Communication Co., Ltd.

Jian Yang

Professor, Dept. of Electronic Engineering, Tsinghua University

SUMMARY

The design of multiple kinds of source information introduces much complexity and a set of challenges in recent signalling systems, but few published methods are applicable to analysis this issue. In this paper, a new inductive approach is proposed based on the model of control theory, in which a set of factors that needs to be in consideration is prompted. A preliminary case study of the proposed approach to Communication Based Train Control system is also presented in this paper to show its effectiveness. Another contribution of this paper is the definition of two basic concepts of source information, which can be extensively adopted by other approaches.

I. INTRODUCTION

The ever increasing complexity of railway signalling systems has brought the challenging task of its safety assurance. One of the complexities in recent signalling systems is contributed by multiple kinds of source information, which is an inherent character of modern railway control systems as the requirement of compound control with multiple modes and reduction of the impact of single fault. This character leads to the issue of information inconsistency, which is hardly avoided because of many factors such as the randomness of communication delay or information process diversity. Risks may arise if there is a lack of careful analysis and elaborated design to maintain system safety.

Therefore, an effective method to conduct safety analysis regarding this issue is needed. However, a good solution is not provided by recent methods. Traditional inductive methods didn't consider such factors, and Fault Tree Analysis (FTA) [1] may lead to state explosion if multiple inputs and mode change are considered in every node of fault tree. An instance is a report released by UNISIG, named Safety Analysis of ETCS Application Level 1 & 2 (SUBSET-088) [2]. It presented the result of safety analysis on ETCS system with FTA, in which the Level 1 and Level 2 control modes are considered independently, and the risks of control mode change are not presented. Hazard and Operability Studies (HAZOP) [3] has been also applied to analyse communication flow, but it is focused on separate information without a clear defined systematic context. Moreover, the traditional methods are mostly based on event-chain model. But for modern systems and their application context, this model has shown its limitations on several aspects to explain accidents or hazards [4].

For reasons stated above, this paper proposes a safety analysis approach with regard to multiple information flow. It's established on the control model proposed in [4]. In this method, a set of factors that needs to be in consideration are prompted, including conflict, partial combination, overlap, blind area, time lag and dynamic change between multiple source information. It forms a new inductive method using the set of factors. Finally, this paper reports a case study of the proposed approach to demonstrate its effectiveness. The control loop based on system theory for a conceptual design of Communication Based Train Control (CBTC) System [5-7] is presented.

In this paper, Chapter II describes two concepts of source information needs in our approach, Chapter III and IV explain the new approach with two steps, and Chapter V is a case study report.

II. TWO CONCEPTS DEFINED ON INFORMATION

Prior to detailed description of the new approach, this section defines two concepts. They reflect essential properties of source information, and form important foundations of our approach. However, these two concepts also can be widely applied on other models and approaches.

Definition A: Common Information Factor

Common information factor (CIF) is defined as two or more source information flows providing the same kind or related message as input of a common process.

This is a symmetrical definition of Common Cause Factor (CCF). When a system is characterized by its physical architecture, CCF is defined as the factor impacting more than one physical module. Symmetrically, when a system is characterized with information flow, CIF denotes that the same kind of message is expressed by more than one information flow.

Morden safety system design can hardly avoid CIF as the consideration of high availability, flexibility and reliability. The typical design introducing CIF includes hierarchy control, multiple mode control and redundant design.

CIF arises on the source information of a model of process, possibly held by controller, actuator or human being (when considered as mental controller with input and output information flow). Figure 1 gives an example of CIF in Chinese Train Control System (CTCS). Under CTCS-2 mode, onboard ATP get moving authorization from track circuit, meanwhile its get such message from Radio Block Center (RBC) under CTCS-3 mode.

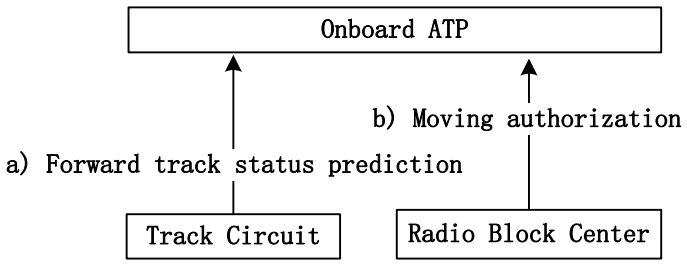


Figure 1: Example of Common Information Factor

Definition B: Information Impact Span

Information Impact Span (IIS) is defined to describe the time duration of source information impact. It's a binary concept denoting whether the source information only has predefined and transient impact span (less than its refresh interval).

A formal definition of IID is presented in this section. Actions of system S is defined by State Equation and Output Equation:

$$\boldsymbol{Y(t) = f(X(t), U(t))} \quad \textbf{(1)}$$

$$\boldsymbol{X(t+T) = g(X(t), U(t))} \quad \textbf{(2)}$$

Here $\mathrm{Y(t)}$ denotes system output information, $\mathrm{X(t)}$ denotes system variables and $\mathrm{U(t)}$ denotes system inputs. T means a specific time lapse.

$\mathrm{U(t)}$ is denoted as "flushed" to target process Pu: $\boldsymbol{U(t): U_f \rightarrow P_u}$ if the following two conditions are both satisfied:

(a) There exists a state equation h, make

$$\boldsymbol{X(t+T) = g\big(X(t), U(t)\big) = h(U(t))} \quad \textbf{(3)}$$

(b) $\mathrm{Y(t)}$ forms "flushed" source information to its target process Py: $\forall \mathbf{y(t)} \in \mathbf{Y(t)}: \mathbf{y_f} \rightarrow \boldsymbol{P_y}$.

If one of the conditions is not satisfied, $\mathrm{U(t)}$ is denoted as "triggered" to target process:$\boldsymbol{U(t): U_t \rightarrow P_u}$.

$\boldsymbol{U(t): U_f \rightarrow P_u}$ means for process Pu, its inner state is only decided by the newest source information, and the earlier message is "forgot" or "flushed by new one". Note "new input" also includes the situation that source information is invalid e.g. communication interrupt.

A signal lamp for the driver on the train is a typical "triggered" message, as once the driver accepts this message and entering approved area, he will not care the subsequent change of this lamp to stop the train: a new message can't "flush" the older one.

III. IDENTIFICATION OF COMMON INFORMATION FACTORS

This section describes how to identify the CIFs in a system, which forms the foundation of analysis presented in Chapter IV.

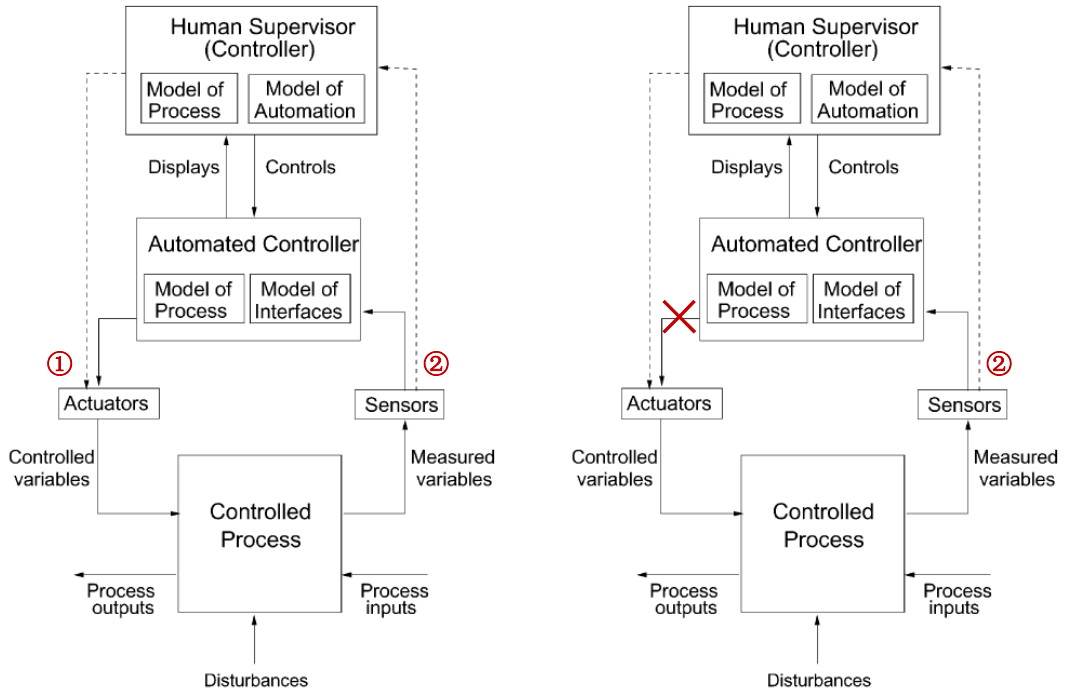
Identification of CIFs is based on the concept of control loop characterizing system actions. Figure 2 (a) shows a typical control loop [4] with the participation of both human supervisor and automated controller. For each module in the control loop, including humans, the controller, actuator, sensors or controlled process/equipment, CIFs can be preliminarily captured by identifying multiple source information flow.

The following structure of control loop shows two potential CIFs from the button up:

(1) CIF of actuator (CIF-1): both human and automated controller control the actuator, which may conflict or overlaps to each other;
(2) CIF of human supervisor (CIF-2): both the sensors (pilot lamp, running state observed by humans) and the displays of automated controller feedback the state of running process. Their inconsistency may confuse the human supervisor and lead to accident.

Note that not all multiple source information forms CIF. For example, the feedback of sensors and the control command from human to automated controller is not considered as CIF, as they bring different messages. Another example is the process input, controlled variables and external disturbances of controlled process. The information flow should be instantiated and analysed in concrete systems.

Another typical type of control loop in safety system is shown in Figure 2 (b). In this system, automation controller not directly acts on the actuators, but only provides aid information to humans. The human supervisor is the unique controller to the actuator. Some arguments consider that the automated controller in this architecture is not safety critical [4]. The CIF analysis shows its unreasonableness: this architecture removes CIF-1 but CIF-2 still exists.



(a) Automation-control structure (b) Automation-aid structure

Figure 2: Two typical control loops of safety-critical system [4]

IV. COMMON INFORMATION FACTOR ANALYSIS (CIFA)

This section proposes possible factors needs be considered on CIFs. For each factor, its common cause and recommended solutions are presented.

(1) Conflict: the same kind of information generated from different source or via different measures, which are commonly applied on safety-critical systems to avoid single-point faults, always prompts the possibility of conflict. Ill definition of the processing strategy may introduce hazards.

(2) Partial combination: this conductive word means each input flow of CIF may be partially used to combine a new one by the controller. It's often happened when each kind of input flow is from more than one source, e.g. information is from a set of onsite units connected to the controller. Risk prompts when there is logical or timing dependence among different unit data.

(3) Overlap: when more than one input flow is expected to control the same object, overlap should be taken into account. It's a common factor in CIF. A good solution to avoid overlap is well definition of controlling interface and keeping consistency of configuration data on different sources.

(4) Blind area: this factor is similar to overlap, but it considers those don't under the control of any object.

(5) Time lag: this factor means different time delay among input flows of CIF. In most cases, it's hard to detect time delay difference from multiple sources. Then there is no way to decide the order of data / events of multiple sources. Possible ways to avoid or reduce its impact include: (1) increase timing tolerance from different sources; (2) safety function doesn't not rely on the event order of different sources; (3) flushed design is recommended to limit the impact of time lag to a tolerant transient.

(6) Dynamic change: a running system may changes in every moment, e.g. change of operation mode, communication states, absence of specific controller and so on. In practical, a well-functioning system under normal conditions often encounters serious problems in external or internal change. The factors of (1) – (5) should be re-analysed under all possible dynamic change conditions.

The consequence analysis for each factor is highly application-dependent. However, the nature of CIF defined in Chapter III helps to determine the impact of a CIF. A flushed CIF normally needs to confirm whether a transient abnormal state (with predicable duration) is acceptable or has been controlled, but a triggered CIF presents comparatively more complicated possibilities. Therefore, the analysis result shows an indication when a triggered CIF appears: it usually needs elaborated consideration and design to avoid possible risk.

V. CASE STUDY ON COMMUNICATION BASED TRAIN CONTROL SYSTEM

This section applies CIFA approach to Communication Based Train Control (CBTC) system up on a traditional interlocking system. The design principle instance of CBTC system comes from IEEE Standard 1474 [5-7].

The presented instance shown in Figure 3 is a partial model of CBTC system, presenting train position determination and moving authorization functions. Other functions are ignored in this case study. In this model, three operating modes are available and can be interchanged with each other: (1) inter-station block mode: traditional interlocking control mode, trains' moving is protected by signals. Only the objects marked with black are active under this mode. (2) Intermittent ATP control mode: trains are protected by ATP system, but only get moving authorities at specific spot. The objects marked with black and blue are active under this mode. (3) CBTC control mode: trains are protected by ATP system, and continuously refresh moving authorities via wireless communication. The objects marked with black, blue and red are active under this mode.

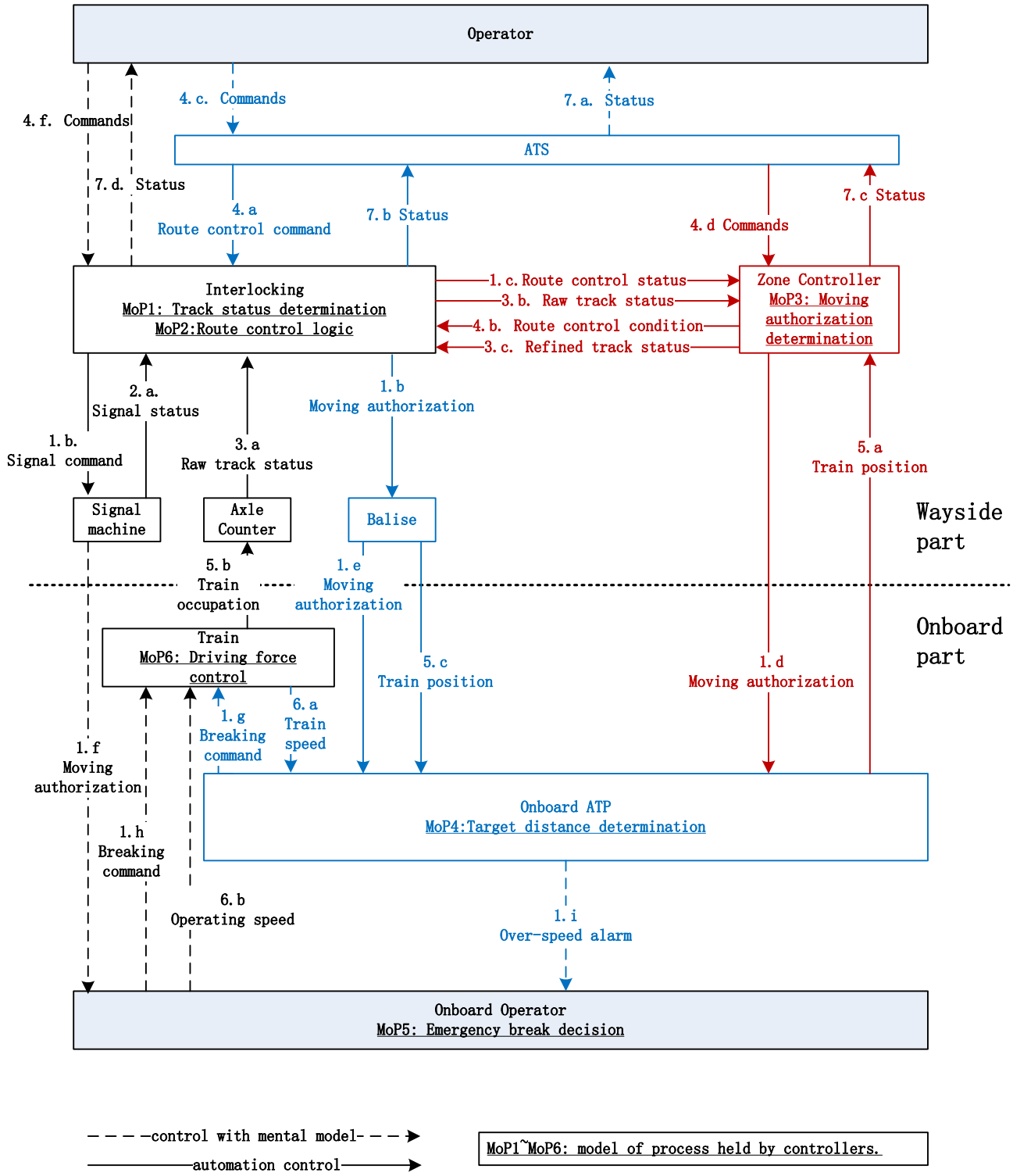


Figure 3: Partial control model of CBTC system

Based on this control model, 6 CIFs are identified following Chapter III and the results are recorded below.

Table 1: CIF identification records

No.	Controller	Mode of process	CIF	Description
CIF-1	Interlocking	MoP1: Track status determination	3.a 3.c	Interlocking system uses raw track status from axle counter and zone controller to generate its own track status.
CIF-2	Interlocking	MoP2: Route control logic	3.a 3.c 4.a 4.b	Interlocking system releases route control according to ATS command, ZC authorization and the track status from axle counter and ZC.
CIF-3	Zone Controller	MoP3: Moving authorization determination	1.c 3.b 5.a	ZC calculates moving authorization for each train according to track status, route control status and train position report.
CIF-4	Onboard ATP	MoP4: Target distance determination	1.d 1.e	Onboard ATP calculates target distance based on moving authorization of ZC and signal authorization from balise.
CIF-5	Onboard Operator	MoP5: Emergency break decision	1.i 1.f	The operator decides if the train should stop according to DMI of ATP and the wayside signal.
CIF-6	Train	MoP6: Driving force control	1.g 1.h 6.b	Train controls the driving/breaking force according to the command of ATP and the driver (operating speed and urgent breaking command).

All identified CIFs are further analysed with regard to its potential hazards and severity. Inductive method is used following Chapter IV. For the space limitation, only a sample of CIF-1 is recorded here.

Table 2: CIF analysis records (sample)

No.	Inductive Cause analysis		IIS	Safety Requirements
CIF-1 Interlocking system uses track status from axle counter and zone controller to generate its own track status.	Conflict	Yes	Flushed	REQ1. Interlocking system should use track status from a pre-defined device, if both ZC and axle counter info are available.
	Partial combination	No		NA
	Overlap	Yes		REQ2. Configuration of track information should keep consistent between ZC and interlocking.
	Blind area	Yes		REQ2. Configuration of track information should keep consistent between ZC and interlocking.
	Time lag	Yes		REQ3. Confusion of track status with maximum T should be acceptable.

No.	Inductive Cause analysis		IIS	Safety Requirements
	Dynamic change	Yes		REQ1. Interlocking system should use track status from a pre-defined device, if both ZC and axle counter info are available.

CONCLUSION

A new risk analysis method was proposed in this paper. To support this method, two important concepts are also proposed to describe the nature of information. The preliminary application of this method on a railway signalling system proves its usefulness in resolve the problems of signalling system introduced by complicated information flow, multiple operation modes and their interchanges.

Future work is planned to establish a complete control model of CBTC or ETCS system and carry out analysis, so as to prove the suitability and effectiveness of this method on systems with different scale and level.

REFERENCE

[1] Roberts N.H., Vesely W.E., Haasl D.F. and Goldberg F.F., Fault Tree Handbook, 1981.Systems and Reliability Research Office of U.S. Nuclear Regulatory.

[2] UNISIG, SUBSET-088, ETCS Application Levels 1 & 2 - Safety Analysis.2002.

[3] CISHEC, A Guide to Hazard and Operability Studies, 1977.

[4] Leveson, N., Engineering a Safer World: Systems Thinking Applied to Safety, The MIT Press, 2012.

[5]. IEEE Std 1474.1-2004, IEEE Standard for Communications-Based Train Control (CBTC) Performance and Functional Requirements.

[6]. IEEE Std 1474.2-2003, IEEE Standard for User Interface Requirements in Communications-Based Train Control (CBTC) Systems.

[7]. IEEE Std 1474.3-2008, IEEE Recommended Practice for Communications-Based Train Control (CBTC) System Design and Functional Allocations.