Reprints

Reprinted From The Chinese Petri Nets Newsletter:

Petri网通讯

第 1 期

On Technical Safety and Security

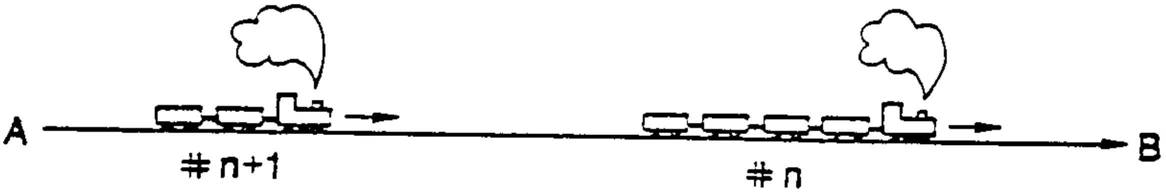
C. A. Petri

March 28, 1989

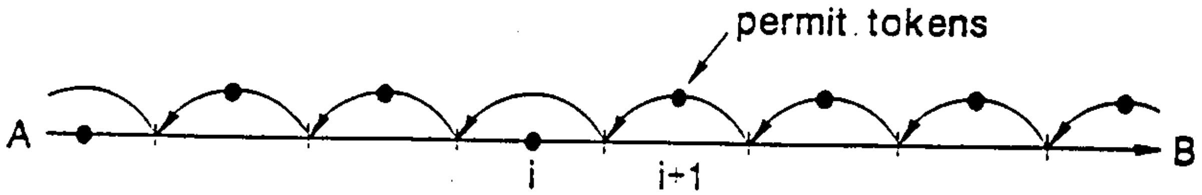
When the first railway trains were put into operation, a man (an quan yuan) had to walk ahead of each train, waving a small red flag and crying "attention! a train!". I laughed heartily when I heared of this for the first time – until it occurred to me that railway traffic was safer at that time than it is now.

Let us study the task of the "safety official" by means of the combinatorics of physical signals, by drawing graphs and nets on which trains and signals may move, represented by small pebbles or "tokens" which denote the presence of trains or signals along a track.

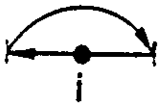
We start with a long one-way track for trains, from A-jing to B-jing:



Train #n might have to stop because a cow is grazing between the rails, or because it has gone out of fuel, or for some other unforeseen reason. Train #n+1 has to be warned in time so that it does not crash into #n. Now a signal which carries the warning might be delayed, also because of an obstacle, or by losing some of its energy. Therefore, warning signals which say "stop as soon as you can" are not a reliable means to prevent accidents. Light signals can be absorbed by mist, etc. Rather, it is more appropriate to the spirit of safety to employ signals not for warning, but for permission. When a train leaves a segment of the track, a signal which permits entry into that segment is put on its way to the next train. Let us describe trains as dots (tokens) moving on a line, and let us segment the line into pieces which are longer than the longest train. No train may enter a segment without the presence of a token of permission:

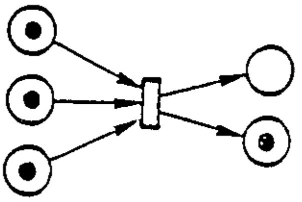


If our graphical (mathematical) model is correct, the trains (and the signals!) are now *safe* in a very precise sense: if every train, in *transition* from segment i to segment i+1, shifts a permit token from the signalling arc i+1 into the arc belonging to segment i, then the number of tokens on each *basic circuit* remains unchanged by all occurrences of



transitions; if this number was one token per basic circuit at the time of construction, it remains 1 as long as the circuit exists, if the Rule of The Token Game is obeyed: A transition of tokens may occur if *all* arcs which point to the transition carry a token; and by the occurrence of a transition, precisely 1 token is removed from the input arcs of the transition, while precisely one token is added to each output arc of the transition.

Then, in our example, there can never be two tokens on the same arc. A marked graph or net with this property is called "safe": it can never happen that all the pre-conditions of a transition are fulfilled while a token is present on one of its output arcs. In a safe net, no situation of *contact* may occur: contact is, as in all traffic, the situation immediately before a crash. In the notation of net theory:



is a <u>contact</u> situation

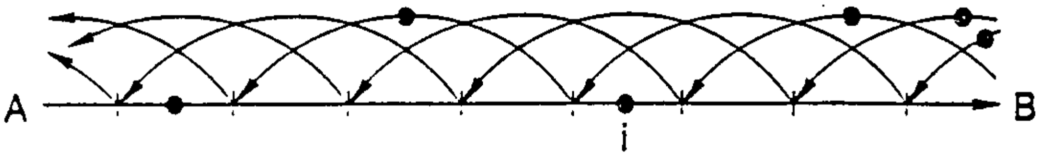
is a contact situation. So in our construction, we have made the net safe by adding a reverse signalling arc to each segment of the track, and putting a signal token (train or permit) onto each basic circuit. The net is safe, the tokens are safe; but are the trains safe?

By no means: our model is not correct in two respects:

1. Real trains have non-zero length. When a train has just entered a segment, it has not yet left the previous segment. Therefore we have to reserve at least two segments for each train, even if every segment is longer than each train.

2. Real trains have non-zero mass. When a moving train finds no permission to enter a segment, it will enter that segment nevertheless; therefore a certain number of segments ahead of the token which represents the signal-transmission-point of the train has to be reserved for the train.

It follows that we have to change the signalling structure in such a way that a (fixed) number of successive segments are reserved for each train: of course, in determining this number, the maximal distance needed for a train to come to a full stop is to be added to the maximal length of the previous train; it is necessary and sufficient to express the result in a number of successive segments to be reserved for each train. Only now it is correct to represent a train by a token. Example:



The token in segment i is now the only token on three (in this example) basic circuits, which overlap in segment i of the track. We had to draw three backward-signalling lines in order to respect length and mass of real trains. The marked graph is safe, and the tokens on the "track" A — B can now represent real trains.

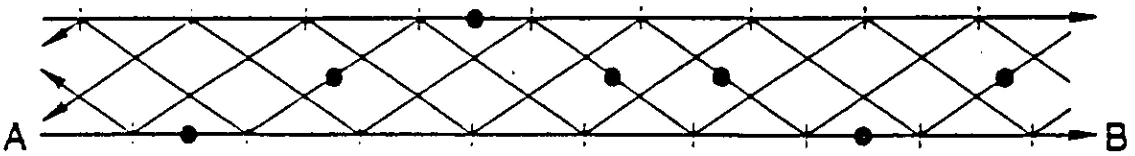
The question is now: can the tokens on the signalling lines represent real signals?

No! Our model is still incorrect in one respect:
Real signals have non-zero length, just like trains (they have to be identifiable as permits).

It follows that we have to reserve for each token which is to represent a real signal at least two consecutive segments of its signalling line. How can we achieve this? In the picture above, only by making sure that consecutive trains have never more than five empty segments between their tokens. That means that the train at i must not reach B before the next train (still near A) has moved.

This might be achieved in two equivalent ways: by coupling consecutive trains by a chain which is short enough, or by introducing additional forward signalling arcs which are long enough. Both ways, we would introduce the absurd constraint that a train would have to stop because the *next* train has to! When we construct a transmission line, we do not want to construct an obligation to transmit; economy requires that trains should be independent (not coupled) so that in times of low demand the schedule can be cut down freely.

In our last picture above, the trains can already move independently with the sole constraint of sufficient separation already satisfied. Only the signals are not sufficiently separated. Here is the simplest supplement to our last construction which fulfils all requirements for trains *and* signals:



By playing the token game, we can easily verify that:

1. Between train tokens, there are always at least two empty segments (one for length, one for mass, i.e. for halting when required.)
2. Between signal tokens, there is always at least one empty segment (for length).
3. The trains are independent (the track A → B may be made empty).
   The marked graph is safe, and no contact can occur, because every segment belongs to a circuit with one token only, i.e. to a basic circuit.
4. On the only forward signalling line (on top of the picture), signals move "in parallel" to the trains: they are not entry permits for trains. Between two of these signals there will always be a train, and between two trains there will always be a "security token" on the top line.

To understand this and to prove it, we must see that our new construction has an additional property which goes beyond safety, and which we call "*security*". The essence of security is, for synchronization graphs, that every *pair of consecutive arcs* belongs to a basic circuit.

This is a requirement which is widely unknown, which in fact looks strange when we see what it means for the relation between trains and permits: trains must be separated from all permits just like trains must be separated from trains and permits from permits!

Yet this is an indispensable requirement of security. Why?

The apparent paradox disappears if we consider transmission lines not for trains, but for electronic messages. These are not different in nature from their corresponding permits and security signals, and the requirement then reads in fact immediately: keep all signals sufficiently separated. We know that *this* is necessary; we are just not accustomed to treat trains like "signals with mass". Remember that we had to respect the mass of trains by *additional* separation between trains; after we have taken care of this, trains *must* be treated like signals in the question of minimal separation (one segment for "length").

Formal proof of security is certainly of high practical value. Two ingredients are necessary:

1. The mathematical model of the real world system must be realistic.
2. It must have the formal property called "security" here.

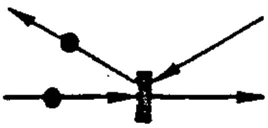
For the latter, we define the notion of "transjunction", short for "con*junction* of conditions across a *tran*sition":

Definition: A transition t is in transjunction in a case c if and only if some input condition and some output condition of t are holding in the case c.

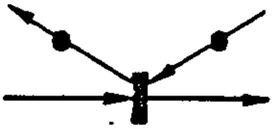
Formally:

$$\text{Transjunction } (t,c) \text{:} \iff {}^{\bullet}t \cap c \neq \emptyset \ \underline{\text{and}}\ t^{\bullet} \cap c \neq \emptyset$$

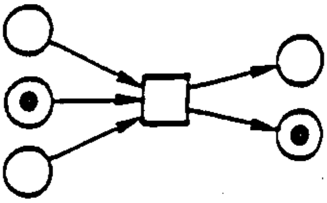
In our pictorial descriptions, examples of transjunction are, in synchronization graphs:



and



in nets more generally:



Finally, we give the

Definition:

An elementary net system or a synchronization graph is **secure** if and only if it has in no case contact or transjunction.

Formally:

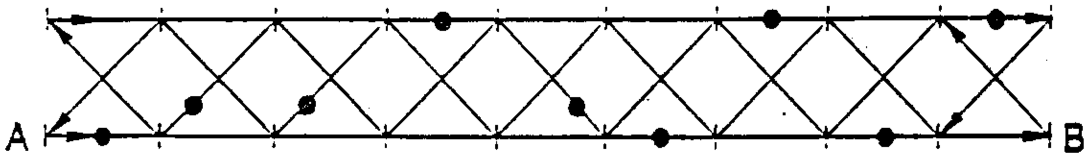
$$\text{Secure}(S,T;F,C) \text{:} \iff$$

$$\bigwedge t \in T, \bigwedge c \in C :$$

$$\left.\begin{array}{lcl} {}^{\bullet}t \subseteq c & - & t^{\bullet} \cap c = \emptyset \\ t^{\bullet} \subseteq c & - & {}^{\bullet}t \cap c = \emptyset \end{array}\right\} \textit{no contact}$$

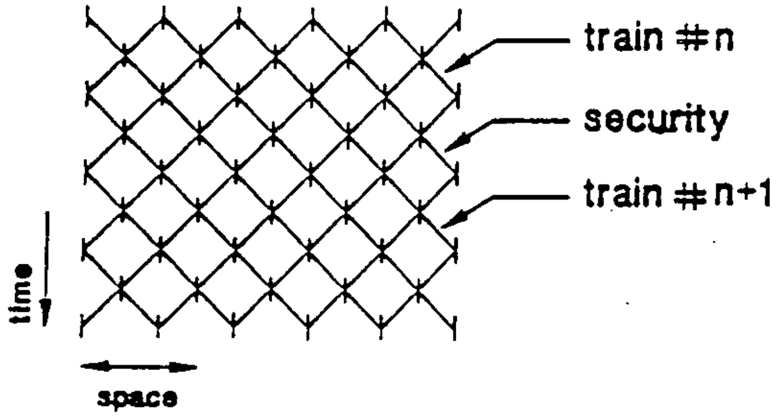
$$\left.\begin{array}{lcl} {}^{\bullet}t \cap c \neq \emptyset & - & t^{\bullet} \cap c = \emptyset \\ t^{\bullet} \cap c \neq \emptyset & - & {}^{\bullet}t \cap c = \emptyset \end{array}\right\} \textit{no transjunction}$$

We showed already the smallest secure transmission line for trains; for "massless trains" like electrical signals the smallest secure transmission line is simpler; it contains two backward-directed lines only.



As required, every transition belongs to *four* distinct basic circuits, because there are four pairings of input/output arcs that must be guarded against transjunction.

We should note that the occurrence graphs of all safe transmission lines shown above, and indeed of all regular secure transmission lines are *identical*, namely:



This insight helps greatly to construct formal proofs of security in general, and also to construct and understand regular secure signalling structures in more than one dimension; while a technical system may be more complex than the two we have considered here, the definition of security and the ingredients for obtaining it remain the same.

Yuan Chongyi helped me to prepare this paper.