METHOD TO MONITOR A PLURALITY OF CONTROL CENTERS FOR OPERATIONAL CONTROL AND BACKUP PURPOSES

The present invention provides a way to automate the hand-off of train control in a rail system and handle failover.
Method to Monitor a Plurality of Control Centers for Operational Control and Backup Purposes

Statement of Related Cases

[0001] This case claims priority of U.S. Provisional Patent Application Serial No. 61/021,855, which was filed on January 17, 2008 and is incorporated by reference herein.

Field of the Invention

[0002] The present invention relates to railways in general, and, more particularly, to a method for controlling train transitions between regional control centers.

Background of the Invention

[0003] Large networks, be they transportation networks or telecommunications networks, often span great distances (e.g., across the U.S., etc.). Due to their size, these networks typically comprise multiple instances of control centers, each of which has a specific geographic or regional zone of influence. A given regional controller is responsible for controlling traffic (e.g., airplane, train, wireless handset, etc.) that is within its zone of influence.

[0004] An issue that arises in all such networks is the transfer or “hand-off” of control responsibilities from one regional control center to the next in conjunction with the migration of the traffic.

[0005] Due to the nature of wireless communications and our very mobile society, hand-off from one wireless “base station” to the next must be computer-controlled and seamless. In transportation networks, the nature of the problem is somewhat different and hand-off is handled with far more operator intervention. In fact, in rail systems, hand off from one controller to the next involves virtually no automation. Furthermore, in rail systems, failover to a redundant system has been handled manually.

Summary of the Invention

[0006] The present invention provides a way to automate the hand-off of control in a rail system and handle failover.

[0007] The inventors recognized that the issues of hand-off and failover are best treated as a single problem; that is, how does a vehicle vitally know with which control center it should be communicating?
The methods disclosed herein operate within the transportation server of each control center. In other words, the method is implemented as software suitable for running on the processor of a transportation server. In accordance with the illustrative embodiment, all relatively static data is stored redundantly at each control center, such that every center has a complete view of the transportation network. This reduces downtime and increases the probability that data is not corrupted in transit. This data is periodically validated between control centers and any modification of the data is immediately transferred to the others, with a positive acknowledgement required.

Dynamic data that is shared between the control center and train is stored only at the responsible control center and on the train itself. If the division between control centers is geographically based, any data that spans the border between control centers is tagged appropriately (e.g., an authority can be granted to a vehicle which exceeds the nominal territory handled by the control center, but it is tagged as “suspect” until validated by the next control center). Any valid control center can send a train the dynamic data so that the train acts independently of the control center with which it communicates. As a consequence, if control moves to a different center, the train will not be affected. An aspect of the illustrative embodiment is to embed information in the messages that are transmitted between a train and control centers so that positive identification is inherent to the messaging (prevents spoofing).

In case of a failure of a control center, the other control centers will notice the failure during periodic validation. Once failure is noticed, the other control centers take over control (upon human confirmation, if so configured). The control centers first determine which vehicles are affected (the vehicles will start to look for another control center when it’s health check fails) and then by uploading all the dynamic data from those vehicles.

**Brief Description of the Drawings**

FIG. 1 depicts a portion of a railway network including two network control centers operating in accordance with the illustrative embodiment of the present invention.

FIG. 2 depicts a method in accordance with the illustrative embodiment of the present invention.

FIG. 3 depicts the portion of the railway network depicted in FIG. 1, wherein one of the network control centers is communicating with the train.
[0014] FIG. 4 depicts a method pertaining to ascertaining the operational status of the two network control centers.

[0015] FIG. 5 depicts the portion of the railway network depicted in FIG. 1, wherein both of the network control centers are communicating with the train.

[0016] FIG. 6 depicts the portion of the railway network depicted in FIG. 1, wherein one of the network control centers is taking control of the territory that is normally controlled by the other network control center.

**Detailed Description**

[0017] The terms below are defined for use in this disclosure and the appended claims:

- **“Vital”** means that a function must be done correctly, or the failure to do so must result in a safe state. Vital is synonymous with “safety-critical.” A safety-critical system is defined when at least one identified hazard can lead directly to a mishap (accident). Standard 1483 (http://shop.ieee.org/ieestore/) defines a safety-critical system as one where the correct performance of the system is critical to the safety, and the incorrect performance (or failure to perform the function) may result in an unacceptable hazard. According to most standards, hazards that have risk ratings of “Unacceptable” or “Undesirable” must be mitigated (i.e., reduce the risk, which is generally done by decreasing the frequency of occurrence) through system and equipment design. In order to do this, all of the functions that are necessary to implement the system must be identified. Functions that have to be implemented so that they are both (1) performed and (2) performed correctly are implemented fail-safely and are identified as “vital” functions. The fail-safely implementation means that all credible failures that could occur are examined and the occurrence of any one of them (or combination of failures in the event that the first failure is not self-evident) maintains the system in a safe state. That can be done either by forcing the system to a stop (or other safe state such as a less-permissive signal) or by transferring control to a secondary system, such as a redundant computer.

[0018] FIG. 1 depicts portion 100 of a railway network. Two territories 102 and 106 are defined within portion 100. Territory 102 is controlled by network control center 104 and territory 106 is controlled by network control center 108. Train 110 is traveling through territory 102 on tracks 112 heading toward territory 106.
[0019] Each network control center 104 and 108 stores all relatively static data, such as the track database, etc. The purpose for this is to minimize downtime and increase the probability that such data is not corrupted in transit (i.e., if the data were not redundantly stored as described herein). This data is periodically synchronized and validated between the control centers (and other control centers that are not depicted in FIG. 1). Any modification of such data is immediately propagated to all network control centers. A positive acknowledgment of the update is required.

[0020] Train 110 is provided with identifying codes for network control centers 104 and 108 (e.g., at installation, etc.). Likewise, the network control centers are provided with an identifying code for train 110. Imbedding the identifying codes in messages between the train and network control centers (or between network control centers) prevents spoofing.

[0021] Dynamic data that is shared between the control center and train is stored only at the responsible control center and on the train itself. This is distinct from the treatment of relatively static data, which is stored at all control centers, as disclosed above. If the division between control centers is geographically based, any data that spans the border between control centers is tagged appropriately. That is, an authority can be granted to a vehicle by a control center for territory that exceeds the nominal territory handled by that control center. But if such authority is granted, it is tagged as “suspect” until validated by nominal control center for the territory in question. Any valid control center can send a train the dynamic data so that the train acts independently of the control center with which it communicates. As a consequence, if control moves to a different center, the train will not be affected.

[0022] If and when a control center fails, other control centers will notice the failure during a periodic validation process. Once failure is noticed, the other control centers take over control (upon human confirmation, if so configured) what would otherwise be the failed controller’s territory. The control centers first determine which particular vehicles are affected and then upload all the dynamic data from those vehicles. Identification of the affected vehicles is based on the fact that it is those vehicles that will start to look for another control center when its health check of the formerly-controlling control center fails.

[0023] FIG. 2 depicts method 200 for controlling a train through a rail network accordance with the illustrative embodiment of the present invention. In accordance with operation 202 of the method, “dynamic” data is transmitted between a train and a first control center. The first control center is nominally responsible for controlling train
traffic within a first territory in which the train is present. “Dynamic” data is defined herein as data that is liable to change on a regular basis, such as authorizations, etc. Dynamic data is distinguished from “static” data, which is defined herein as data that is not likely to change on a regular basis, such as a track map, etc. Also, in contrast to static data, which is stored at all control centers, dynamic data is shared only between (and stored only at) the train and the controlling control center.

[0024] The dynamic data is stored on both the train and at the first control center, as per operation 204. In accordance with operation 206, a second control center is notified that the train is in the first territory, wherein the second control center is responsible for controlling traffic within a second territory that is adjacent to the first territory. In the illustrative embodiment, the first control center notifies the second control center of the presence of the train in the first territory.

[0025] In operation 208, the first control center issues a grant of provisional authority to enter the second territory. This grant is considered suspect until validated by the second control center, which nominally controls the second territory.

[0026] In operation 210, the second control center grants the train full authority to enter the second territory when it is determined that it is safe to do so. At this point, the train will still be in the first territory. The second control center issues no other control messages until the train enters the second territory.

[0027] FIGs. 3, 5, and 6 depict the practice of method 200 in the context of portion 100 of the railway system of FIG. 1.

[0028] FIG. 3 depicts communication between network control center 104 and train 110. The train verifies that all messages come from a control center having a known identification code. Likewise, network control center 104 verifies that all messages it receives come from a train having a known identification code. Additionally, network control center 104 verifies the crew of the train via a logon or password.

[0029] Furthermore, network control centers 104 and 106 communicate. In particular, and among any other messages, control center 104 advises control center 106 of the existence of train 110 in territory 102. Furthermore, control center 104 sends a message to control center 106 advising that it (control center 104) granted provisional authority to train 110 to enter territory 106. The purpose for the provisional grant is to reduce the likelihood that train 110 will be forced to stop before the “handoff” to control center 106 occurs.
[0030] Additional communications between the control centers 104 and 106, and between the control centers and a train, include the transmission of a “heart beat.” The heart beat is intended to gauge the health of the control center. FIG. 4 depicts this process.

[0031] In accordance with operation 402, a first signal is transmitted from a first control center to a second control center, wherein the first signal is indicative of the operational status of the first control center.

[0032] A second signal is transmitted from the first control center to a train, wherein the second signal is indicative of the operational status of the first control center, as per operation 404.

[0033] A third signal is transmitted from the second control center to the first control center, wherein the third signal is indicative of the operational status of the second control center, in accordance with operation 406.

[0034] A fourth signal is transmitted from the second control center to the train, wherein the fourth signal is indicative of the operational status of the second control center, as per operation 408.

[0035] Using this method, it can be determined which, if any, of the first or second control center is having operational difficulties. This is discussed further in conjunction with FIGs. 5 and 6.

[0036] FIG. 5 depicts train 110 nearing territory 106. Control centers 104 and 108 send and receive heartbeats, as per method 400. Furthermore, train 110 sends location reports to both of the control centers. Train 110 will enforce the limits of its authority (i.e., it will stop) unless any control center (other than control center 104) validates the provisional authority granted by control center 104.

[0037] In FIG. 5, network control center 108 communicates with approaching train 110 and grants full authority for the train to enter territory 106 as long as it is safe to do so.

[0038] FIG. 6 depicts a scenario in which control center 104 fails. Network control center 108 loses the heartbeat from control center 104. Control center 108 then communicates with train 110 to verify their loss of contact with control center 104. Once verified, control center 108 takes control over territory 102, which was formerly controlled by control center 104. Control center 108 continues to use its own copy of static data, but retrieves all dynamic data from any trains that were under the control of control center 104 at the time the heartbeat was lost.
[0039] It is notable that train 110 might not be directly aware of the failover of control center 104 since the train simply validates messages that come from valid control centers; it does not have knowledge, *per se*, of the control center that originates the message.

[0040] It is to be understood that the disclosure teaches just one example of the illustrative embodiment and that many variations of the invention can easily be devised by those skilled in the art after reading this disclosure and that the scope of the present invention is to be determined by the following claims.
What is claimed is:

1. A method for controlling the movement of a train through a rail network, wherein the rail network comprises a plurality of territories, and wherein a respective plurality of control centers control traffic within the territories, wherein the method comprises:
   transmitting dynamic data between the train and a first control center that is responsible for controlling traffic within a first territory in which the train is present;
   storing the dynamic data on the train and at the first control center;
   notifying a second control center that the train is in the first territory, wherein the second control center is responsible for controlling traffic within a second territory that is adjacent to the first territory;
   granting the train provisional authority to enter the second territory, wherein the first control center issues the grant of provisional authority; and
   granting the train full authority to enter the second territory when it is determined that it is safe to enter the second territory, wherein the second control center issues the grant of full authority and wherein the second control center issues no other control messages until the train is within the second territory.

2. The method of claim 1 and further comprising:
   transmitting a first signal from the first control center to the second control center, wherein the first signal is indicative of the operational status of the first control center;
   transmitting a second signal from the first control center to the train, wherein the second signal is indicative of the operational status of the first control center;
   transmitting a third signal from the second control center to the first control center, wherein the third signal is indicative of the operational status of the second control center; and
   transmitting a fourth signal from the second control center to the train, wherein the fourth signal is indicative of the operational status of the second control center.

3. The method of claim 2 and further comprising verifying, with the train, loss of contact with the first control center when the second control center does not receive the first signal.
4. The method of claim 3 and further comprising assuming control of the first territory when loss of contact is verified, wherein the second control center assumes control.

5. The method of claim 4 and further comprising retrieving dynamic data from the train at the second control center once control is assumed thereby.
Transmitting dynamic data between a train and a first control center, wherein the first control center is responsible for controlling train traffic within a first territory in which the train is present.

Storing the dynamic data on the train and at the first control center.

Notifying a second control center, which is responsible for controlling train traffic within a second territory, that the train is in the first territory.

Granting the train provisional authority to enter the second territory.

Granting the train full authority to enter the second territory when it is determined that it is safe to enter the second territory.
Transmitting a first signal from a first control center to a second control center, wherein the first signal is indicative of the operational status of the first control center.

Transmitting a second signal from the first control center to a train, wherein the second signal is indicative of the operational status of the first control center.

Transmitting a third signal from the second control center to the first control center, wherein the third signal is indicative of the operational status of the second control center.

Transmitting a fourth signal from the second control center to the train, wherein the fourth signal is indicative of the operational status of the second control center.
### A. CLASSIFICATION OF SUBJECT MATTER

**INV. B61L27/00**

According to international Patent Classification (IPC) or to both national classification and IPC

### B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

B61L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic database consulted during the international search (name of database and, where practical, search terms used)

EPO-Internal, WPI Data

### C. DOCUMENTS CONSIDERED TO BE RELEVANT

<table>
<thead>
<tr>
<th>Category</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>WO 96/33899 A (WESTINGHOUSE BRAKE &amp; SIGNAL [GB]; CLIFTON RAY [GB]; SADLER STEVE [GB];) 31 October 1996 (1996-10-31) page 15, line 27 - page 16, line 27 page 40, line 7 - line 11 figures 4,5</td>
<td>1-5</td>
</tr>
</tbody>
</table>

For further documents, see the patent family annex.

* Special categories of cited documents:
  * **X** document defining the general state of the art which is not considered to be of particular relevance
  * **E** earlier document but published on or after the international filing date
  * **L** document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
  * **O** document referring to an oral disclosure, use, exhibition or other means
  * **P** document published prior to the international filing date but later than the priority date claimed
  * **T** later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
  * **X** document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
  * **Y** document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
  * **A** document member of the same patent family

**Date of actual completion of the International search**

8 April 2009

**Date of mailing of the international search report**

20/04/2009

**Name and mailing address of the ISA/**

European Patent Office, P.B. 5816 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax (+31-70) 340-2016

**Authorized officer**

Massalski, Matthias
<table>
<thead>
<tr>
<th>Category</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>DE 27 22 396 A1 (SIEMENS AG) 23 November 1978 (1978-11-23) page 11, line 6 - line 34 page 13, line 10 - line 22 figure 1</td>
<td>1-5</td>
</tr>
<tr>
<td>A</td>
<td>DOSSMANN W ET AL: &quot;VERNETZUNG VON RZUE-ZENTRALEN&quot; SIGNAL + DRAHT, TELZLAFF VERLAG GMBH. DARMSTADT, DE, vol. 84, no. 6, 1 June 1992 (1992-06-01), pages 172-178, XP000297104 ISSN: 0037-4997 the whole document</td>
<td>1</td>
</tr>
<tr>
<td>A</td>
<td>WICKINGER T: &quot;SICHERER DATENAUSTAUSCH ZWISCHEN DEN INTEGritaETSBEREICHEN VON BETRIEBSZENTRALEN&quot; ETR EISENBAHnteCHNISCHE RUNDSCAU, HESTRA-VERLAG, DARMSTADT, DE, vol. 50, no. 6, 1 June 2001 (2001-06-01), pages 355-359, XP001206493 the whole document</td>
<td>1</td>
</tr>
<tr>
<td>Patent document cited in search report</td>
<td>Publication date</td>
<td>Patent family member(s)</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>----------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td>EP 0970868 A</td>
<td>12-01-2000</td>
<td>CN 1508036 A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WO 9841435 A1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>JP 3269635 B2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DE 69420101 T2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EP 0650429 A1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>JP 7507752 T</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WO 9426571 A1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AU 704058 B2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AU 5404196 A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CA 2219756 A1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DE 69610494 D1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DE 69610494 T2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DK 822909 T3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ES 2152018 T3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>HK 1003630 A1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NO 974962 A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PT 822909 E</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 5947423 A</td>
</tr>
<tr>
<td>EP 1510430 A</td>
<td>02-03-2005</td>
<td>AT 318745 T</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DE 10336022 A1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FR 2391100 A1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GB 2445374 A</td>
</tr>
</tbody>
</table>