

---

## **Collaborative workspace**

**(a common electronic information platform for the rail sector)**

**having the purpose of increasing Safety and Efficiency and reducing Cost in the Fragmented Railway System**

### **A. Summary - the idea**

A Collaborative Workspace (CW) is the use of a Cyberspace database/repository system via the Internet which is hosted by a neutral organisation in terms of ensuring that sufficient server capacity capable of handling any form of document/data is available. It would also ensure that a **push messaging system** is available for notifying registered involved/interested parties of any new or amended document/database occurrences affecting their notified interest within that database/repository system.

Such a workspace ensures that updated information will be available on an ongoing basis and the users need not – as now – search a great number of Internet sites or magazines to get the information they need. The user can get it from one place and he will immediately and automatically be informed when new information in the field that he subscribes to is available.

The information could be placed either in a public area or in a restricted area open only to those subscribers defined by the information supplier. Information that might be placed on the CW could be: all legal regulations, OTIF technical specifications (APTU Annexes), TSIs, standards, instruction and maintenance manuals, warnings for safety problems with specific constructions or spare parts, information on new products and working methods, etc.

The costs of running the system should basically be covered by the parties who subscribe to get notifications and retrieve information. The information providers should in principle pay no fee for placing their information on the CW.

The idea is generated by UIP and this document has been drafted in co-operation between UIP and the OTIF Secretariat, Technology/Approval section.

### **B. Background**

The advent of Interoperability of the railway system, as perceived, will occasion widespread fragmentation, immediately removing the interface of one control authority (national RUs) with two entities (customers and suppliers) and by default replace it

with a multitude of interfaces which increase exponentially with each new entrant to the system.

Regulations and technical specifications from OTIF and EU are being introduced with the intention of establishing a framework of regulatory measures covering the obligations and liabilities of the Railway Undertakings (RUs) as Train Operators (duty holders), the private keepers of rail vehicles, infrastructure managers (IMs) and other parties in the railway business to operate safely. Naturally, where appropriate, obligations and liabilities cascade down from the duty holders to their customers and suppliers to ensure that the duty holder meets his safety obligations.

The situation of the freight operating companies is especially complicated as they have to contend not only with their own equipment/suppliers but must also take into account the equipment of the customers and their chosen suppliers/maintenance regimes. This additional variance is complicated by the fact that customers and their freight wagons are nomadic. The liability of the duty holder does not change however and he must ensure that all wagons in his train conform either by in-house auditors or through accredited third party auditors.

The problem arising from the foregoing will manifest itself when RUs and wagon owners/keepers and their equipment suppliers begin to experience that demands for audit on them rise. Time and cost associated with this exercise will escalate, thus increasing the cost of rail transport with no added benefit.

### **C. Additional Industry Problems Noted**

Railway Safety Cases and technical specifications (OTIF APTU Annexes and TSIs) will undoubtedly have situations which on paper are apparently ensuring safety but in reality are often physically, under the present constellation, impossible to fulfil or if being fulfilled involve delay, unnecessary time/cost implications and uncertainty by many parties as to whether they are fully compliant, in spite of their time/cost efforts and could therefore be exposed unknowingly in a court of law following any incident which may warrant that step.

By way of example:-

- (i). Vehicle keepers will be required to have knowledge of wagon engineering certificates and to be able to monitor any limitations included in them. Effectively this is a physical impossibility in the nomadic environment of freight wagons without reference to a central database.

- (ii). All users of the rail system are required to meet the OTIF APTU Annexes technical standards and the TSIs.
- (iii). For any company to try to remain up to date compliant under point (ii). means continual reference to lists to ascertain changes etc., and then onward distribution to all interested parties within the company.
- (iv). Safety Critical component manufacturers establish their limits or amend them as experience demands but how do end users/their maintainers know that they are working to the latest limits? A recent situation revealed, perchance by an owner using three different maintenance companies for the same axlebox, that they were working to three different rejection/acceptance limits with each believing they had the latest requirements!

The foregoing is indicative of the Pandora's box awaiting opening by the first serious incident.

#### **D. The Requirement**

Ideally interested parties should have direct access, on a real time basis, to the information on the databases of all parties concerned or be directly informed by those parties of all additions/changes to their products, services or standards. Clearly it would not be acceptable to the companies supplying information to permit users of their information/products to have direct access to their databases, not forgetting that the variation in systems and formats used could be a nightmare for both parties in linking in.

The cost of undertaking to keep all interested parties informed would not be inconsiderable and then there is always the problem of the limited field of distribution and the need to verify that information has been received where legal liability exists in this respect.

Clearly companies could decide to pass their information to a central managing database company to manage the process but this involves all of a company's work being made available and possible error in the conversion/entry to the central database. Again companies are not prepared to lose direct control over their data and have extra cost in that direction. Thus not all companies would be keen to participate and the aim of the project would be lost.

#### **E. A Considered Solution – Collaborative Workspace**

Collaborative Workspace is the use of a Cyberspace database/repository system via the Internet which is hosted by a neutral organisation in terms of ensuring that suffi-

cient server capacity capable of handling any form of document/data is available. It would also ensure that a push messaging system is available for notifying registered involved/interested parties of any new or amended document/database occurrences affecting their notified interest within that database/repository system. The host does not participate or have access to what is placed in the system; i.e. the detail in the system is controlled only by the originator/author of the detail placed into the system. The originator/author continues to use and control his own database/information system and only posts to the repository in the format he uses. The repository automatically ensures that the appropriate viewer operates when the repository is accessed by an authorised party via his Internet Browser.

The repository logs when and by whom any data is deposited, altered and accessed. It retains copies of data/documents before and after alteration and by whom accessed so that traceability is at all times available. The traceability system is accepted by the law courts.

Users of the system have only to register with the participating companies with whom they have an interest to verify their level and acceptability of interest/level of information to which they should have access and are password coded accordingly. Thus the supplier of information has control over who may receive his information and to what level. The system automatically registers the user to receive a push email whenever the information area, for which he is registered, is posted/amended/superseded and so on. This means that the user does not have to continually check his information sources and the supplier of the information only needs to post the information in the repository once. The moment the user views the information push email notified to him, a receipt notification is recorded in the system. The supplier therefore has an immediate confirmed receipt.

The validation of the user can be set to whatever each individual supplier on the system requires. For example:-

1. No validation at all - detail available to all and sundry - open access (e.g. to public information).
2. Subscriber ID and Password allocated by the information supplier – not open access but with a risk of abuse.
3. Digital signature status issued by, for example, Royal Bank of Scotland using the same security process employed for Internet Banking whereby the Bank effects all verification checks to ensure that the user is definitely the one known and accepted by the supplier of information.

Naturally it could be agreed by all participants registering their information in the repository that the system under point 3. be used by them all since the verification needs only to be effected once. Once validated into the repository the user is then automatically graded to his level of viewing/interaction agreed by each supplier. The system under point 3. is also an easy method of blocking access by withdrawing the digital signature should any abuse of the system be suspected, until checked.

## **F. Benefits**

The advantages of the Cyberspace repository are:-

1. Information is available on a real time basis.
2. The supplier of information remains in full control of his data and does not need to change his existing in house data format.
3. The supplier of information retains control over the users accepted by him and their access levels.
4. The supplier of information only posts information once. He does not have to worry about delivery to the end user and verification of receipt. The push email system and logging of access to individual items of information controls this aspect.
5. Errors are quickly remedied by posting corrected versions and again the user is made immediately aware by the push email notification system. Verification of receipt again logged by the system.
6. Consultation Papers can be posted. Consultees notified by push email. Consultees may make their comments, which are traceability logged and available for all other consultees to view. Thus the whole consultation process is more secure and simplified.
7. No special knowledge or equipment is required by the user. Only Internet access with a normal browser – Internet Explorer or Netscape – and registration with information supplier is required.

## **G. Examples**

All legal regulations, OTIF technical specifications in the APTU Annexes, the TSIs, standards, instruction and maintenance manuals, warnings of safety problems with specific constructions or spare parts, information on new products and working methods, etc., could be posted in the repository and all consultations conducted within the

system. Changes, new issues or deletion/superseding of this information would be made immediately known to users with record of receipt logged. Minutes of meetings, seminar papers and emergency notifications can all be entered into the system. The volume/cost of printing, postage and mailroom staff is reduced effectively to zero but availability of information is immediate and ongoing and is coupled with receipt logging and acceptance of the system by courts of law where liability may exist to inform etc.

All vehicle engineering acceptance certificates on vehicles can be immediately posted when issued and thereby RUs and keepers have automatic access to such detail with any time or engineering limitations.

It can be imagined what other organisations in the rail industry would save in ensuring that their end users are kept up to date whilst having the knowledge that the system has legal backing.

The cyberspace repository system described above represents an easy to set up system which can bring the fragmented rail industry together in appropriate information sharing of all information, particularly safety critical information, on a real time basis with considerable savings in printing and distribution/checking costs. It allows control to remain in each company's hands and has legal acceptability. Because of its ability to deal with all types of information and formats and its easy access via the Internet it can be used for all purposes and individual groups can join together to create their own villages if they so require.

Collaborative Working in the Cyberspace environment as described is perhaps the fastest method of furthering increased **Safety, Efficiency and Cost in the Fragmented Railway System**