Assuring EULYNX: Application of CSM-RA to Specification Development

Stephen Bull[a]

Ebeni Limited
Corsham, UK

David Shipman[b]

Network Rail
Birmingham, UK

Abstract *EULYNX is developing the specifications for standardised technical interfaces for railway signalling systems across multiple European railway infrastructures. We have successfully established an assurance approach, based on CSM-RA, to assure the interface specifications. Using CSM-RA aligns EULYNX to the acceptance processes within the countries where the interfaces will be used. Assurance of EULYNX aims to give confidence to product developers that products using these interfaces will be acceptable on railways across Europe. We have completed an initial baseline of the assurance and are now extending this to consider further details of the EULYNX interfaces*

1 The aim of EULYNX

The EULYNX Consortium comprises a number of European Railway Infrastructure Managers[1] (IMs), including the largest UK IM, Network Rail, working together to develop and maintain a modular architecture and standardised technical interfaces within and between railway signalling systems. This enables separation and extension of component lifecycles, thus opening markets, accelerating

[a] Stephen is a Principal Safety Engineer and can be contacted at stephen.bull@ebeni.com

[b] David is Innovations Engineering Manager with the Signalling Innovations Group and can be contacted at david.shipman@networkrail.co.uk

[1] Infrastructure Managers are the organisations charged with establishing and maintaining the fixed railway infrastructure, including track, signalling and control systems.

innovations, and achieving economies of scale. This is achieved through development of common specifications for each interface that align to the needs of each individual IM.

The details of these interfaces vary significantly between different railways and even different suppliers, usually driven by the historic development of national standards. The benefit of standardising interfaces is that the IM has freedom to choose from all the products available on the market to select the most appropriate solution for their application. Standardisation of interfaces also reduces the costs of approvals and assurance, because a greater part of these activities need be undertaken only once, when the interfaces are first developed.

2 Achieving standardised interfaces

2.1 Architecture

Within a railway signalling system the interlocking is the high-integrity equipment which ensures that trains are kept safe. The interlocking is the central "brain" of the signalling system, which receives commands for train movements from a control system: it then determines whether these commands can be enacted safely (dependent on the positions of trains and on the other movements which have been permitted) and issues permission for trains to move (in the form of trackside signals or direct communication to the driver's cab).

The interlocking ensures that:

- permission for trains to move is only given when safe
- trains permitted to move are protected from other trains
- points, moveable infrastructure and other interfaced equipment is only operated in accordance with safety requirements

The EULYNX development is not changing the architecture of the signalling system; instead, it is focussed on the specification of standard interfaces between railway interlockings and the surrounding objects (e.g. train detection system, points, and signals); the functionality of the objects themselves is not addressed by EULYNX (except in certain limited cases). The EULYNX development is based on the system architecture shown in Figure 1. The main technical interfaces are between the interlocking and:

- adjacent interlocking
- train detection system
- light signal
- points

- control system
- radio block centre
- level crossing
- track worker safety system
- other generic I/O devices

The architecture distinguishes between:

- control interface (SCI)
- diagnostics interface (SDI)
- maintenance interface (SMI)

The architecture also distinguishes between:

- subsystems – partly within the EULYNX system boundary; the EULYNX specifications may include some aspects of the functionality for these subsystems as well as a pure specification of the interface
- adjacent systems – wholly outside the EULYNX system boundary; the EULYNX specifications only specify the interface

The scope of the EULYNX development is limited to developing and assuring the interface specifications, covering only Phases 1-5[2] of the CENELEC system lifecycle defined in (EN50126-1 2017); the Consortium itself is neither developing products nor applying them to the railway.

The interfaces are developed using a Model Based System Engineering (MBSE) approach using SysML; executable subsets of the model are developed to support validation of individual interfaces.

2.2 Baselines

The development of EULYNX is structured into a number of baselines. Baseline 2 was initially published in December 2017 and provided a complete specification of a major subset of the interfaces up to and including sequence diagrams defining interface behaviour. These diagrams were also verified against the IMs' requirements.

Baseline 3, due for publication in 2018, will extend the EULYNX specification to further interfaces, and include the development of the State Machine models which provide for validation of the interfaces by the IMs.

Further baselines will be published as required, in order to complete coverage of all interfaces and address any feedback from implementation of EULYNX-enabled equipment, particularly in conjunction with early adopter projects including those in Germany, The Netherlands and Norway.

[2] Phase 5 is only partially covered by EULYNX.

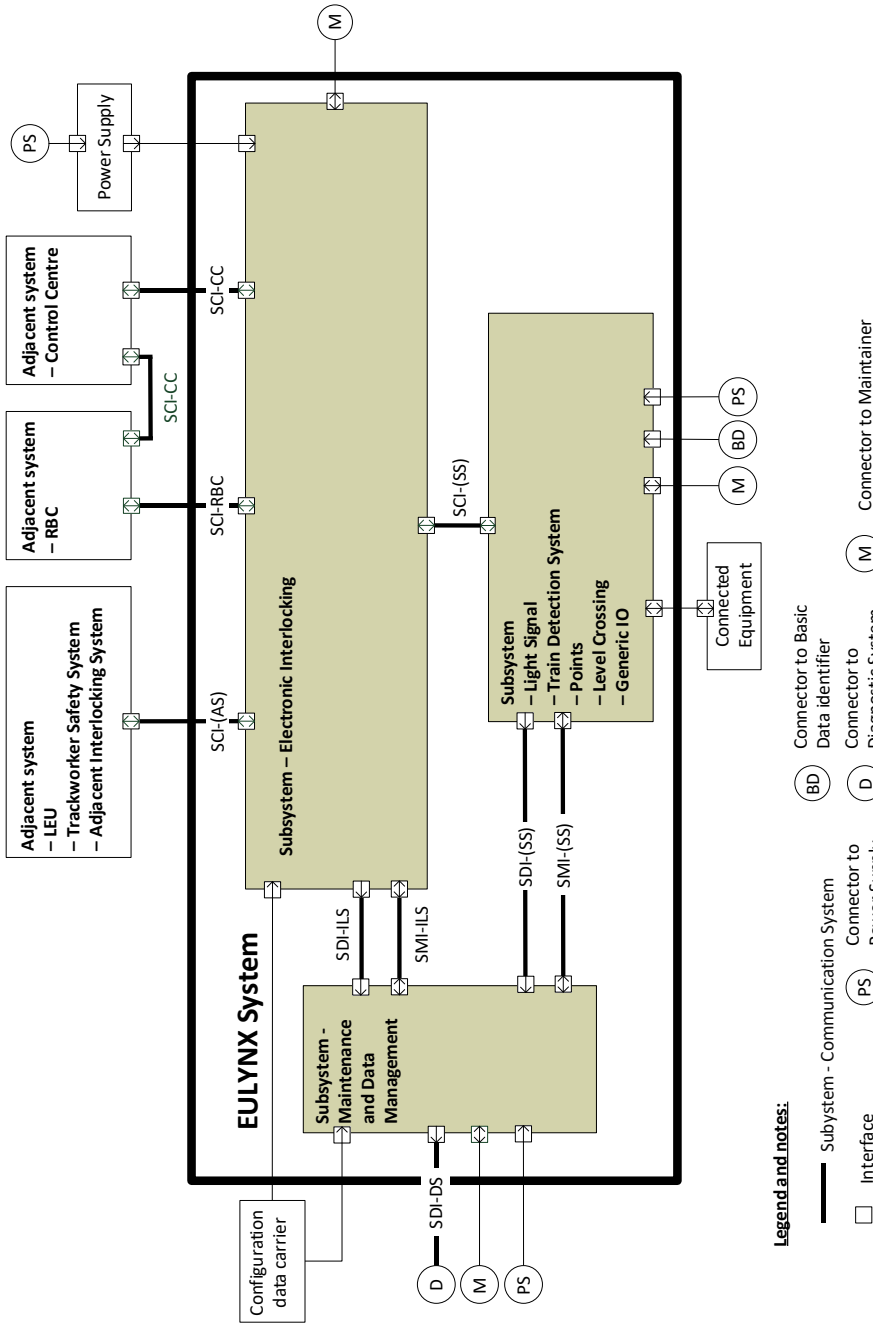

Fig. 1. EULYNX System Architecture

2.3 EULYNX Consortium

For the first three years, leading to Baseline 2, EULYNX operated as a project to deliver the core outputs. From the end of 2017, EULYNX became a standing organisation, a consortium of IMs from twelve countries across Europe. The Consortium is overseen by a Consortium Management Committee (CMC) consisting of representatives from all participating IMs. There is also a Steering Committee which represents the governance level and is attended by senior representatives of the IMs. The consortium continues to manage the ongoing development through Baseline 3 and into the future maintenance phase.

2.4 Assurance

We are assuring the EULYNX specifications so that these assurance activities do not need to be repeated for every product development which implements EULYNX interfaces. It is intended that this assurance will be made available as a "black box" to support product assurance.

3 Challenges in assuring EULYNX

The main challenges in assuring EULYNX are:

- aligning the assurance to (only) the scope of the EULYNX specification development
- the choice and application of a suitable set of standards for assurance
- the different standards and perspectives of the twelve IMs
- the arrangement of the EULYNX Consortium into clusters responsible for delivery of individual artefacts
- ensuring the assurance was valid for envisaged applications
- the division of EULYNX delivery into a series of baselines
- the need to consider both safety and assurability[3]
- the tension between safety and security

[3] Assurability here means the sufficiency of process and evidence to demonstrate that the required safety (and other) properties of the system are achieved.

3.1 Aligning assurance to scope of development

EULYNX specifies the interfaces between the interlocking and other systems: the functional behaviour of the signalling system is controlled by the interfaced products. The EULYNX specifications are largely restricted to the content of the messages and the mechanisms for ensuring their safe communication. Assurance has been approached in two phases: first limited to the control interfaces; then adding subsystem functionality and other interfaces.

The EULYNX development only addresses the early phases of the system lifecycle, i.e. Phases 1-5 in (EN50126-1 2017), with interface specifications as the output. Assurance is limited to the development of those specifications. If the (V model) development of the railway application is a "big-V", EULYNX assurance is only concerned with a "little-v" in the top left of the "big-V". This is illustrated in Figure 2.

Our challenge was to assure the whole EULYNX development, without needlessly overlapping with existing assurance processes.

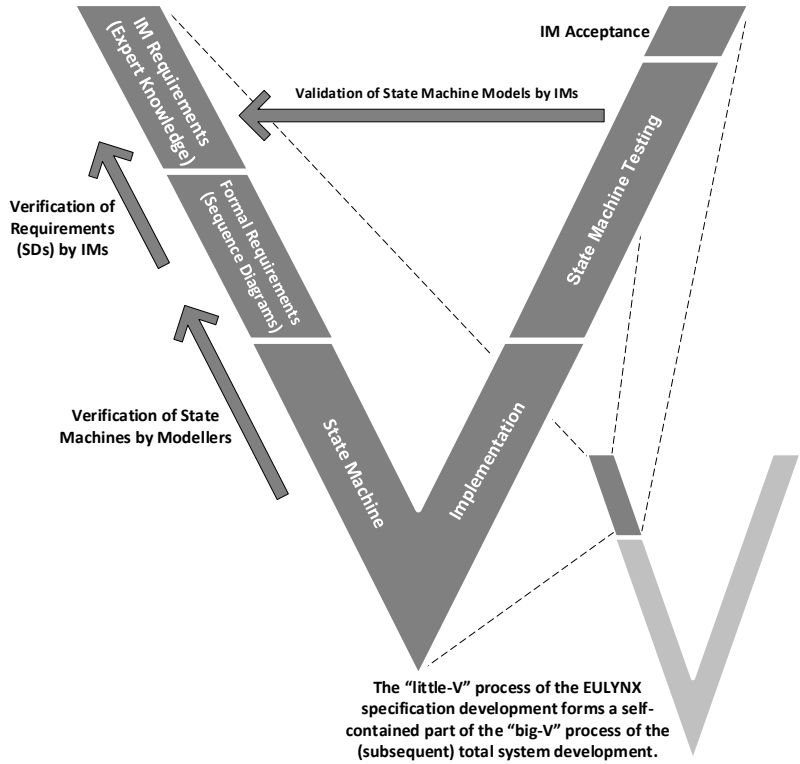

Fig. 2. "Big-V" and "Little-v" V&V processes

3.2 Applying a suitable underlying standard

The purpose of assuring EULYNX is to allow the specifications to be applied in product development in confidence that they will be acceptable for application on a wide range of railways. The EULYNX assurance is intended to be a "black box" component which supports the assurance of products without needing further analysis of the EULYNX specifications, which could lead to inconsistent application through "preferential[4]" challenges. We therefore needed to base the assurance on an established standard acceptable to all EULYNX IMs and their National Safety Authorities (NSAs).

The Common Safety Method for Risk Evaluation and Assessment (CSM-RA) (CSM-RA 2013) is the method prescribed for risk assessment of change to the railway system within any European member state; it was therefore natural to assure EULYNX using CSM-RA because it provides a rigorous framework accepted by all the EULYNX IMs. Consequently, application of the process should generate assurance in a form acceptable to those IMs with minimal modification of their acceptance processes.

However, CSM-RA assumes that its application is to a change to the system, whereas EULYNX is only covering one part of the system change (which would include the application of the product incorporating EULYNX interfaces). Therefore the challenge was to apply CSM-RA to the limited scope discussed in section 3.1, reflecting the "little-v" in Figure 2.

3.3 Different approaches between IMs

The EULYNX IMs are of varying size (ranging between Luxembourg and Germany), complexity and population density. Consequently the standards and approaches applied by the IMs vary significantly to meet the needs of their individual railways. The IMs also vary in the maturity of their application of formal safety management processes: some have a lot of experience (and resource) to contribute to the EULYNX specifications, others are receptive to the expertise and experience of the more established railways.

The EULYNX assurance had to establish a process acceptable to all the IMs and their NSAs; we also had to allow for the variety of approaches and standards applied by the different IMs. (E.g. some IMs do not require their interlockings to achieve the highest level of system integrity: EULYNX assurance must support, but not enforce, the highest level of integrity.)

[4] The concept of preferential engineering is a common factor in the railway industry (as in others), whereby changes are demanded that do not affect the overall outcome, but simply represent a preferred alternative approach.

Throughout this it must be remembered that EULYNX is not the highest decision-making authority – each IM has ultimate responsibility and accountability to their own NSA.

3.4 Diversity of clusters

The EULYNX Consortium is arranged into a number of working groups known as clusters. As well as clusters for each interface, there are core clusters which address the overarching issues of: System Architecture, Modelling & Testing (including systems engineering processes), Security and Assurance. In addition, the Data Preparation cluster is developing a standardised data model for exchange of (geographic) data between IMs and suppliers; this cluster largely sits apart from the others.

Participation in each cluster is open to all members of the consortium, although not all members are actively represented in every cluster. Participants in the clusters are considered to be highly experienced in their fields, drawn from multiple locations and groups within those IMs; their participation must be managed alongside their own day-to-day priorities which can sometimes constrain their EULYNX contribution.

A key challenge was therefore to develop an assurance regime that was consistent across the diverse clusters, and took account of the varying participation from different IMs.

3.5 Applicability for envisaged applications

Although the EULYNX specifications assume the architecture shown in Figure 1, there is no requirement for an IM to apply the EULYNX specifications to all its signalling system interfaces. An IM could choose to apply EULYNX only at a single interface type (e.g. between the interlocking and the light signals) and / or for only some examples of an interface type (e.g. between one interlocking and an adjacent one, particularly likely where other adjacent interlockings might not be EULYNX ready).

The challenge was to ensure that the assurance will remain valid for such partial applications of the EULYNX specifications.

3.6 EULYNX Baselines

EULYNX is being developed in a series of baselines as described in section 2.2. The first phase of the assurance has been undertaken on Baseline 2, focusing on the control interface specifications, and followed publication of the baseline. As the EULYNX development matures towards Baseline 3, we are extending the assurance to include subsystem functionality and diagnostic and maintenance interfaces. In particular:

- the interfaces are being modelled as executable state machines to support their validation: these state machines did not form part of Baseline 2
- other interfaces will be assured if and when they are developed (planned for after Baseline 3)

The challenges were:

- to provide assurance which is as complete as possible for the published baseline, while also clearly identifying the further work required
- to achieve convergence between development and assurance so that assurance for future baselines is completed concurrently with the publication of the baseline

3.7 Safety vs Assurability

In addition to *hazards* (i.e. situations which could result in an accident on the railway), we also consider *assurance threats*[5] (issues which threaten the assurability of the EULYNX specifications, typically requiring action to address potential inadequacy of the argument or available evidence). These are important, because the aim of the assurance is to provide a body of evidence which supports the later acceptance of products applying EULYNX.

The challenge was to manage these hazards and threats in an integrated way.

3.8 Interfacing safety and security

Cyber security is a growing concern in all critical industries. As we rely increasingly on networked communications, across networks which are (a) increasingly used for multiple purposes and (b) use COTS equipment, we are increasingly

[5] Subsequent mentions of threat refer to *assurance* threats, unless an alternative meaning is given.

exposed to risk of attack. Security measures must rapidly adapt to emerging security threats, opportunities and technologies, without undermining the fundamental safety justification. At the same time there must be a sufficient security framework for the overarching safety requirements to be clearly addressed.

Arising from the different timescales for the safety and security lifecycles, the challenge is to provide stable safety assurance to support product development and acceptance while also being sufficiently flexible to react to emerging security threats; cyber security is considered as a cause to safety hazards as explained later.

4 Addressing the challenges

We addressed the challenges described above as follows:

- clear definition of **scope**, covering:
  - technical scope (i.e. initially limited to the interfaces)
  - lifecycle phases
  - EULYNX baseline
- application of the **Common Safety Method** for Risk Evaluation and Assessment
- use of a single **clearly defined approach** to identify and manage hazards and threats
- use of a **combined record of hazards and threats** including details applicable to individual clusters where required
- ongoing **consultation** with clusters
- security through application of **suitable protocol** and development of security concept

Comparison between the list above and the list of challenges identifies how each of the challenges has been addressed.

4.1 Definition of scope

In our assurance plan we defined the EULYNX assurance scope, mindful that our system boundary was more than just architectural, and that the functionality (and hazards) of an overall signalling system and its components are well established:

- the EULYNX system boundary is only a subset of the signalling system
- EULYNX only deals with Phases 1-5 of the system lifecycle

Our main task is to assure that any message entering one end of the interface is accurately transmitted to the other end in a timely manner. Our scope definition helped to avoid getting drawn into analysing the functionality described in the messages which pass over the interfaces: this would have duplicated work which is (rightly) undertaken when analysing the functions of the products and the signalling system.

4.2 Application of CSM-RA

4.2.1 Introduction to CSM-RA

Many readers will be familiar with Common Safety Method for Risk Evaluation and Assessment (CSM-RA 2013) and there are several good sources of guidance[6] to its application. In essence it comprises the following steps:

- proposal of change
- significance decision
- system definition
- hazard identification
- risk evaluation and acceptance
- safety requirements
- safety justification

These steps are supplemented by ongoing processes of planning, hazard management and independent assessment. The CSM-RA process integrates into a wider framework for monitoring safety on the operational railway, as described in Taking Safe Decisions (RSSB 2014).

CSM-RA defines three risk acceptance principles (RAPs) which can be used to accept the risk associated with a hazard:

1. Codes of Practice – i.e. appealing to existing standards to mitigate the risk
2. Reference Systems – i.e. appealing to the safety requirements for a comparable system which is already in operation
3. Explicit Risk Estimation – i.e. undertaking a detailed assessment of the risk and demonstrating that the identified safety requirements reduce the risk to an acceptable level

The CSM-RA aims to harmonise processes for risk evaluation and assessment and the evidence and documentation produced during the application of these processes. By applying a common process, it is intended to make it easier for an

[6] For example: (ERA 2009) (ORR 2015) (RSSB 2017)

assessment undertaken in one EU Member State to be accepted in another with the minimum of further work (mutual recognition).

4.2.2 CSM-RA is the natural choice

CSM-RA appears to be the natural choice because:

- All European Member states are required to apply CSM-RA to changes which are made to their railway infrastructure, and they have already adapted their acceptance processes to align to the approaches taken by CSM-RA.
- Any application of the EULYNX specifications (in the EU, at least) will eventually need to be subject to the CSM-RA.
- CSM-RA produces assurance which can easily be used as a "black box" to support assurance of product development and application.

Our application of CSM-RA is supported by using CENELEC standards as Codes of Practice - in particular (EN50126-1 2017) (EN50126-2 2017) (EN50129 2003) (EN50159 2010) - to demonstrate that the risks identified have been suitably controlled. It is interesting to note that the CENELEC standard on railway safety assurance (EN50126-1 2017) (EN50126-2 2017) now adopts the same RAPs as CSM-RA.

4.2.3 Challenges in applying CSM-RA

We needed to interpret CSM-RA to assure EULYNX, meeting the principles while tailoring the application to unique circumstances; this is because CSM-RA is primarily focused on assessing the risk of an actual change to the railway, whereas the EULYNX specifications form only part of the process of developing a product which in turn is part of a bigger change.

The biggest challenges were in determining whether the CSM-RA RAPs were sufficient, and to integrate *threats* into the process:

- **Risk Acceptance Principles (RAPs)**: we considered adding additional RAPs, because we expected to identify risks which could not, at the specification phase, be controlled by the standard RAPs. We initially proposed three additional RAPs, although ultimately they were not developed further as the standard three RAPs were found to be suitable in every case:
  - **Engineering Judgement**: Judgement made by a quorate group of suitably qualified and experienced personnel that the risk is controlled to a level at least as good as achieved for similar systems
  - **Application Requirements**: Risk controlled by placing requirements on subsequent phases of development or application.

  - **Architectural Change**: Risk controlled by change to the architecture.

- **Explicit Risk Estimation (ERE)**: We were concerned that, if we needed to apply this RAP, it would be difficult to calibrate risk definitions which would be acceptable to all IMs. In the event, the only appeal to this RAP is qualitative and has not been contentious. In part, this is assisted by an *a priori* decision that all the control interfaces should be generically capable of SIL4[7] integrity, removing any question of specific safety levels for individual interfaces. (SIL4 is chosen because this highest level of integrity is expected for many signalling products.)
- **Threats**: from the outset we expected to identify a number of issues which were not safety risks (and therefore could not be sensibly described as hazards), but which threatened the *assurability* of the EULYNX interfaces: these were captured as *threats*: the same principles were applied to mitigating the risks from these threats, except that they were not assigned RAPs.

4.2.4 Development processes to assure integrity

As noted above, all the control interfaces need to be capable of supporting functionality at SIL4. This means that even in the early phases of the system lifecycle, sufficient rigour must be applied to the development, in order to support a later claim to have achieved a particular SIL.

We reviewed the CENELEC standards, in particular (EN50126-1 2017) (EN50126-2 2017) and (EN50129 2003) to identify a suitable set of processes to control the risks and to achieve the required integrity level. This set of processes aligned closely with those already defined in the EULYNX process documentation: as a result, we were able to confirm that the processes applied by EULYNX are suitable to support a claim of SIL4 integrity when products (and applications) are developed which incorporate the EULYNX interfaces.

4.3 Use of a single clearly defined approach

Our approach uses the following steps:

- Undertake hazard identification (HAZID) with representatives of the clusters
- Analyse output of HAZID sessions to identify hazards, hazard causes and threats and populate a hazard record

[7] In accordance with (EN50126-2 2017)

- Identify how the risk represented by the items in the hazard record would be managed, by identifying a series of
  - assurance requirements (ARs) to be demonstrated by the EULYNX development; and
  - safety-related application conditions (SRACs[8]) to be demonstrated by applications of the EULYNX interfaces
- Identify the owner(s) of the assurance requirements within the EULYNX Consortium, and the evidence required to demonstrate compliance with those assurance requirements.
- Confirm with each cluster which ARs and SRACs applied to their scope of work, and that they accepted the evidence requirements
- Gather the evidence to demonstrate (in the Assurance Justification Report) that the risks are suitably managed.

The outputs are reviewed by an independent Assessment Body (as required by CSM-RA): an initial review of the process and plan confirms the suitability of the approach, followed by observation of the process and review of the Assurance Justification Report to confirm that it has been applied correctly.

The process is illustrated in Figure 3.

Our HAZID was undertaken as a series of generic sessions; taken together these gave a cross section of representation from the clusters. Although there was no single session with representatives from all the clusters, there was sufficient interaction and representation to give a quorate HAZID.

In the first phase of assurance, we focussed just on the interfaces. As we were not assuring the *content* of the interfaces, the issues identified were common to all interfaces. This led to a relatively simple set of hazards, hazard causes and threats, which were largely common across the whole development. As a result, although we originally envisaged separate HAZIDs for individual interfaces, these were not needed for the first phase.

However, in the latest phase, we are in the process of running specific HAZIDs and identifying issues relating to the functionality of the subsystems.

[8] SRAC is the term often used in safety cases, for conditions which must be satisfied by the application, in order for the conclusions of the safety case to be valid. Not all our conditions are directly *safety*-related, because some are managing threats rather than hazards, but we have retained the term for consistency.

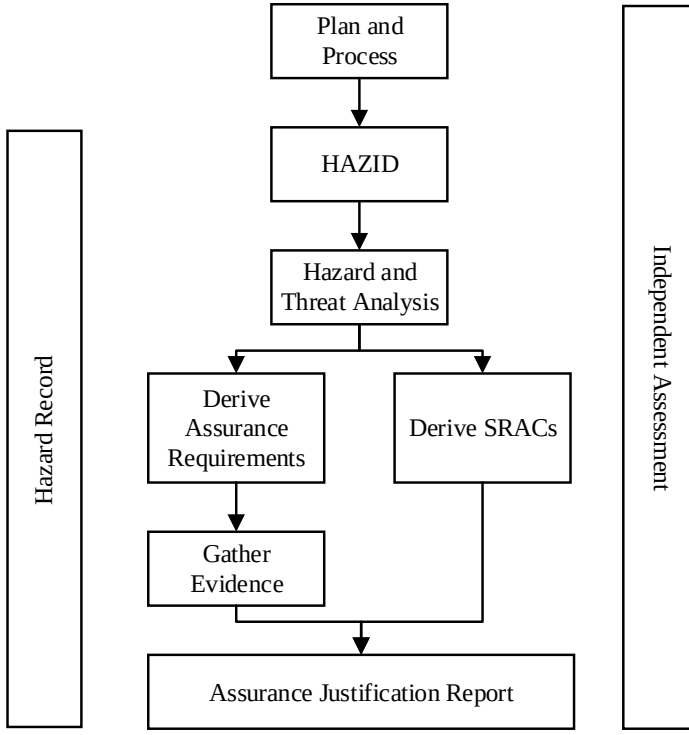

Fig 3. EULYNX Assurance Process

4.4 Use of a single record of hazards and threats

We identified only three high level hazards (compared with around twenty on a typical railway resignalling project). At this stage of system development, management of the threats is just as important, to ensure that the final system will be assurable. We managed threats within the hazard record with the same level of rigour as hazard causes, although we did not assign RAPs to threats.

Once we had established our set of hazards, hazard causes and threats, we identified ARs and SRACs to manage the risks. The process of assigning these to clusters and reviewing them is described in the next section.

Although we have used a combined hazard record, we have clearly identified variations between clusters. This has allowed us to identify a set of requirements and conditions for each of the EULYNX interfaces, thus allowing identification of the relevant subset of requirements where only a subset of the EULYNX architecture is applied.

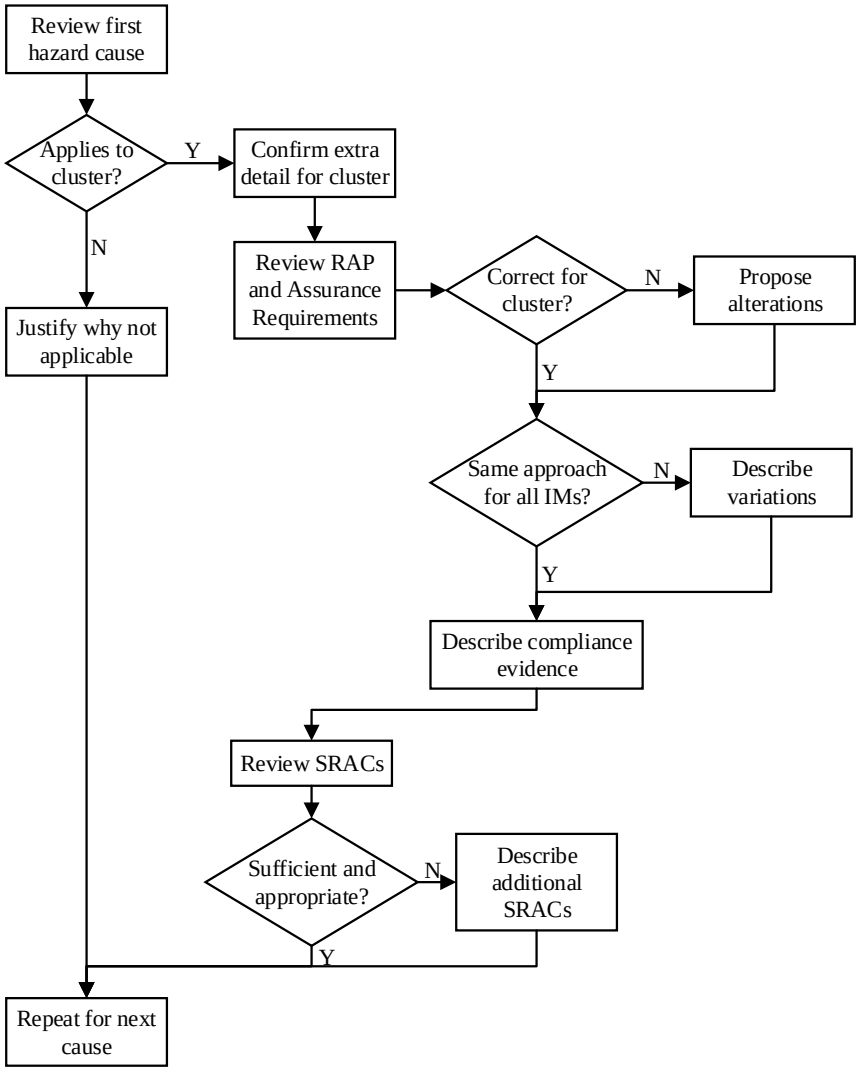

Fig. 4. Process for clusters to respond to proposed allocation of hazard causes– a similar process was used for response to allocation of threats

4.5 Ongoing consultation with clusters

We extracted the information from the hazard record into worksheets presenting the information relevant to each cluster. We prepared a separate worksheet for

each hazard cause and for each threat and requested that each cluster should review our proposals and either confirm acceptance or propose modifications. This is illustrated in Figure 4. The worksheet included the applicability to the cluster, the proposed ARs, the proposed supporting evidence, and the proposed SRACs. This gave the cluster members an accessible means of reviewing the elements of the hazard record relevant to them; they also had the hazard record available for reference.

Comments from the clusters were reviewed collectively and final responses agreed. Any concern over the level of cluster engagement was managed transparently with full awareness and support from the lead representatives of all IMs. Each IM was aware of the risks to them of insufficient participation.

4.6 RaSTA protocol and security concept

At a fundamental level, EULYNX is using the RaSTA[9] protocol (DKE 2015) for safety-critical communications: this provides the protections expected by (EN50159 2010), giving confidence that communications are sufficiently protected when deploying the interfaces across a category 2 network[10]. It is left to the Security Concept to demonstrate that the infrastructure provided is equivalent to a category 2 network.

However, this is not enough in a field which is evolving and changing so quickly. EULYNX has formed a Security Cluster whose remit is to develop a security concept which will allow IMs to effectively combat security threats without necessitating constant changes to the equipment and interfaces, which necessarily have a much longer lifecycle of change, and without requiring changes to the safety justification that would prevent additional or altered security measures being implemented in a timely manner.

It is intended that the implementation of this concept will be integrated into existing efforts by the IMs. The impact of this concept on the EULYNX interfaces will be monitored through liaison between the Security cluster and the other clusters, including the Assurance cluster.

We will adopt the HAZID process described earlier to undertake an assessment of the security threats. This will identify any security issues which must be managed within the safety work, and to confirm whether a category 2 network plus the RaSTA protocol provides sufficient protection.

[9] RaSTA: Rail Safe Transport Application

[10] (EN50159 2010) defines a category 2 network as: "open transmission systems where, although the transmission is not fully under the control of the safety-related system designer, the risk of malicious attack can be considered negligible"

5 How well did it work?

We set out to provide assurance of EULYNX, such that product and application developers would be able to use the specifications with confidence. We have made significant progress towards this goal:

- We have established a **process, based on CSM-RA**, by which the EULYNX development can be assured in a way which will be acceptable to all participating IMs and NSAs.
- We have identified a **core set of hazards, hazard causes and threats** which cover the EULYNX interfaces.
- We have identified **Assurance Requirements** (to be satisfied by the EULYNX development, to manage the risk as far as possible) along with supporting **evidence required** to demonstrate that these requirements have been met; we have also gathered and referenced a significant amount of this evidence.
- We have identified **Safety-Related Application Conditions** which need to be met by anyone applying the EULYNX specifications – these represent risk controls which cannot be implemented by the EULYNX development itself.
- Independent assessment of our work has commenced.

Our findings are summarised in the EULYNX Baseline 2 Assurance Justification Report (AJR) which has been approved by the EULYNX CMC; at this phase the AJR identifies the further steps required to achieve our goal of declaring that "the EULYNX Specifications are fully assured[11]": these are summarised in the conclusions of this paper. The final AJR will be used by the IMs as part of their wider system assurance case; the SRACs will be published for suppliers to comply with.

5.1 What did we find?

We identified just three hazards at the boundary of our scope (i.e. states of the part of the system specified by EULYNX which could cause an accident). The hazards are listed in Table 1.

[11] Naturally, this assurance is only valid where the specifications are used as specified within the EULYNX architecture and in accordance with the published constraints.

Table 1. EULYNX Hazards

Hazard	Description
HAZ-0001: Interface does not communicate information correctly	An incorrect message is transmitted across the interface to the receiving product. Correct input is corrupted by the interface, resulting in incorrect output. We identified a range of potential causes, including those identified in (SCSC 2018), all of which lead to the same hazard.
HAZ-0002: Interface is insufficiently available	No message is passed across the interface
HAZ-0003: Incorrect information is provided to the interface	Message provided to interface contains incorrect information. This message may be: in a valid format, but incorrect or in an invalid format

We identified six hazard causes and thirteen threats to the assurability of the system. Our hazards, hazard causes and threats were mostly generic – i.e. equally applicable to each of the interfaces specified by EULYNX. The generic nature of the hazards is not unexpected, given that the Baseline 2 analysis covered the interfaces themselves. The assurance of subsystem functionality (in Baseline 3) is in the process of uncovering more specific hazards. We identified Assurance Requirements (ARs) and Safety-Related Application Conditions (SRACs) to control the risks from the hazards and threats.

We found that the risk (where it is under the control of the EULYNX development) is controlled by the processes by which EULYNX develops the interfaces. Note that, although the evidence might be delivered by the cluster responsible for the interface, the process applied is defined by the overarching clusters: Architecture, Modelling & Testing, and Assurance.

We were able to demonstrate good alignment between the processes which the CENELEC standards recommend for system development (at the lifecycle phases within EULYNX scope) and the processes employed by the EULYNX consortium.

The main mitigation against incorrect communication is the RaSTA protocol (DKE 2015) adopted by the programme as the underlying protocol to be used by all the control interfaces. This protocol provides the protections required for a category 2 network, and has been adopted by EULYNX for each of the control interface specifications.

5.2 Application of Common Safety Method

CSM-RA provides a suitable framework to identify hazards, hazard causes and threats relating to the development of interface specifications.

Despite early concerns, we found that the standard CSM-RA RAPs (primarily Codes of Practice and Reference Systems) were sufficient; we did not need to appeal to the proposed extra principles. (It became apparent in early reviews that it would anyway have been difficult to gain acceptance from the IMs for any additional principles.)

The main Codes of Practice which we applied were the CENELEC standards (EN50126-1 2017) (EN50126-2 2017) (EN50129 2003), plus the ISO/IEC System Engineering Standard (ISO/IEC15288 2015) as sources of accepted processes with which to manage the risks which we identified.

5.3 Different perspectives

The development of application conditions was particularly interesting because it revealed significant differences between the expectations of different IMs. Two application conditions stand out:

- **Safety Integrity Level (SIL)**: We started out with an assumption that the interfaces will process information with the highest level of integrity (SIL4). However, not all applications require SIL4. The result is that EULYNX requires interfaces to be *capable* of supporting SIL4 applications and each application must complete a risk assessment to determine the integrity required.
- **Category 2 network**: The RaSTA protocol (DKE 2015) used by the control interfaces assumes that the messages will be sent over a network which is category 2 as defined in (EN50159 2010). Not all IMs are able to provide a category 2 network across their whole railway, especially on railways in remote areas. The EULYNX assurance currently requires these IMs to demonstrate that they have provided functional equivalence to a category 2 network. It is envisaged that once suitable reference systems have been reliably demonstrated, the EULYNX specification might evolve to explicitly include these alternatives, removing an element of bespoke assurance for IMs in the future.

5.4 Volume of information

The main challenge to managing the hazard record arose because, although the hazards, hazard causes and threats were largely generic (i.e. applicable to each interface), some clusters took a slightly different approach in how they interpreted the risk and in the evidence which was provided to demonstrate control of the risk. The variety in the response received from the clusters provided benefit by giving a more comprehensive understanding of the risks than would have otherwise been possible.

Each cluster's response was recorded separately within the hazard record to ensure that the full breadth of perspectives was captured. This initially gave a separate variant of the hazard record for each cluster, which led to a significant overhead in processing the information returned. For later baselines we intend to put additional effort into reconciling these, although we recognise that a small number of variations will undoubtedly remain.

5.5 Issues common to many other projects

The following issues are common to many (if not all) engineering projects:

- **Establishing competence**: hazard identification and review is only valid if it has been undertaken by a quorate set of competent people: rather than attempt to establish a competence framework specific to EULYNX, we proposed that it is the responsibility of the IMs to provide team members competent in the relevant disciplines to provide input on the relevant interfaces on their IM's behalf, and that the diversity of involvement across so many IMs provided additional mitigation of any risk; this proposal was endorsed by all IMs through the CMC.
- **Establishing quoracy**: it is not feasible for every IM to be represented in every cluster (including every interface). Even where clusters nominally have members from a wide range of IMs, a large proportion of the active involvement comes from a much smaller core group. We established the principle that material developed by a cluster would be circulated to all members, with a deadline to respond: non-response was then considered to be acceptance by default, another principle which has been accepted by the EUYLNX CMC.
- **Common understanding of terms**: it is critical in an engineering project that technical terms are understood with the same meaning by all participants. This is particularly relevant where participants are from:
  - different railways, where different signalling principles are applied
  - different cultures, with different approaches to acceptable risk
  - different native languages – for example, in several European languages, the same word is used for "safety" and "security", whereas these have distinctly different meanings in English

  The project maintains a glossary which provides the agreed EULYNX definition for technical terms. A particular concern is where the meaning of a term may differ between IMs (or between application contexts). The glossary is critical to define the formal EULYNX definition for a term and it is important that this glossary is understood and used correctly by all participants. The glossary has been reviewed from an assurance perspective to identify any potential impact on safety from the way in which the terms have been defined.

6 Conclusion

We have successfully established a basis for assuring EULYNX, both in terms of an agreed and accepted process and an accepted (minimal) set of hazards, hazard causes and threats. This was achieved by unifying a wide range of disparate inputs into a consolidated hazard record. We established a simple process for clusters to engage with the hazard record, giving them the information which they need in a form which is easy for them to review – although we recognise that we need to improve the process of incorporating responses from clusters into the hazard record in a harmonised way.

We have successfully completed the first phase of assurance, resulting in acceptance of the Assurance Justification Report for Baseline 2 by CMC. Further work to be undertaken during the Baseline 3 assurance includes:

- completion of evidence to support the argument as it stands – this includes validation evidence from executable state machines being developed to model the interfaces
- further analysis of areas which were excluded from the Baseline 2 assurance, including:
  - additional interfaces, in particular the Track Worker Safety System
  - functionality of the EULYNX subsystems, in particular: train detection, points, light signal
  - functionality of the diagnostics and maintenance interfaces, which use a different protocol from the control interface
- apportionment of cyber security threats between safety and security
- completion of independent assessment (the Assessment Body role under CSM-RA) to provide confidence to any projects applying the specifications that the work to develop them has been suitably assured and does not need to be revisited - we had intended that our work would be independently assessed before the completion of the Baseline 2 assurance; this assessment is still ongoing at time of writing.

Acknowledgments This paper is based on work undertaken by Ebeni Limited as Assurance Consultant to the EULYNX Consortium, under contract to Network Rail who are the lead for Assurance work on behalf of the Consortium. We acknowledge the support of the individuals and organisations involved in the Consortium who have helped us to shape this approach and who have supported us in assuring EULYNX. We acknowledge the permission given by the Consortium to publish this paper. We also acknowledge the detailed work undertaken by Zoë Alderman of Linnaeus Enterprises in delivering the project and her invaluable comments on various drafts of this paper.

References

CSM-RA (2013) EU 402/2013, Commission Implementing Regulation No 402/2013 on the common safety method for risk evaluation and assessment, as amended by EU 2015/1136, Official Journal of the European Union, 2013

DKE (2015) DIN VDE V 0831-200 (VDE V 0831-200):2015-06 Electric signalling systems for railways – Part 200: Safe transmission protocol according to DIN EN 50159 (VDE 0831-159), DKE German Commission for Electrical, Electronic & Information Technologies of DIN and VDE, 2015

EN50126-1 (2017) BS EN50126-1:2017, Railway Applications. The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS). Generic RAMS Process, CENELEC, 2017

EN50126-2 (2017) BS EN50126-2:2017, Railway Applications. The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS). Systems Approach to Safety, CENELEC, 2017

EN50129 (2003) BS EN50129:2003, Railway applications. Communication, signalling and processing systems. Safety related electronic systems for signalling, CENELEC, 2003

EN50159 (2010) BS EN50159:2010, Railway applications. Communication, signalling and processing systems. Safety-related communication in transmission systems, CENELEC, 2010

ERA (2009) ERA/GUI/01-2008/SAF Guide for the application of the Commission Regulation on the adoption of a common safety method on risk evaluation and assessment, Version 1.1, European Railway Agency, 2009

ISO/IEC15288 (2015) ISO/IEC15288, Systems and software engineering -- System life cycle processes, ISO, 2015

ORR (2015) Common Safety Method for risk evaluation and assessment – Guidance on the application of Commission Regulation (EU) 402/2013, Office of Rail Regulation (now Office of Rail and Road), 2015

RSSB (2014) Taking Safe Decisions - How Britain's railways take decisions that affect safety, Rail Safety and Standards Board, 2014

RSSB (2017) GE/GN8646 Guidance on the Common Safety Method for Risk Evaluation and Assessment, Issue 1, Rail Safety and Standards Board, 2017

SCSC (2018) Data Safety Guidance, Version 3.0, Safety Critical Systems Club Data Safety Initiative Working Group, 2018