PRACTICAL EXAMPLES ON CSM-RA

Common Safety Method:

- What for?
- How?

SUMMARY

CSM-RA
A short history summary

CSM-RA understanding
What is there to be done?

CSM-RA example of application
Practical examples for each step

Conclusion
Is CSM-RA totally new work?

CSM-RA

A short history summary

Why the CSM-RA

- History of railways:
  - Multiple historical Railway Undertakings in Europe (more than 100 years of railway history)
  - Typically one “big” historical Railway Undertaking per country (Public Company, due to merging of multiple private companies which where not always economically self-sufficient)
  - Each company was responsible of its safety (self validation / acceptance of modifications, including new trains)

- European Union => European Railways:
  - Creation of the European Railway Agency to promote/ensure Interoperability between the countries of Europe
    - Creation of a National Safety Authority for each country to ensure independence between the operator and the authorisation (and thus ensure fairness in authorisation for other operators)
    - Creation of Technical Specifications for Interoperability to provide the essential requirements to ensure interoperability (these requirements are common to all countries, and out of the scope of NSAs => fairness in authorisation for other operators)
  - However:
    - Ensuring interoperability does not ensure a coherent level of safety (mostly out of the scope of TSIs)
    - Each Railway Undertaking & each NSA have different means of achieving safety (e.g. different documents to be conform to, different numerical criteria, …)
  - Creation of the Common Safety Method on Risk Acceptance to ensure that a safety demonstration will be valid in all countries (if safety study still applicable to the country)

CSM-RA understanding

What is there to be done?

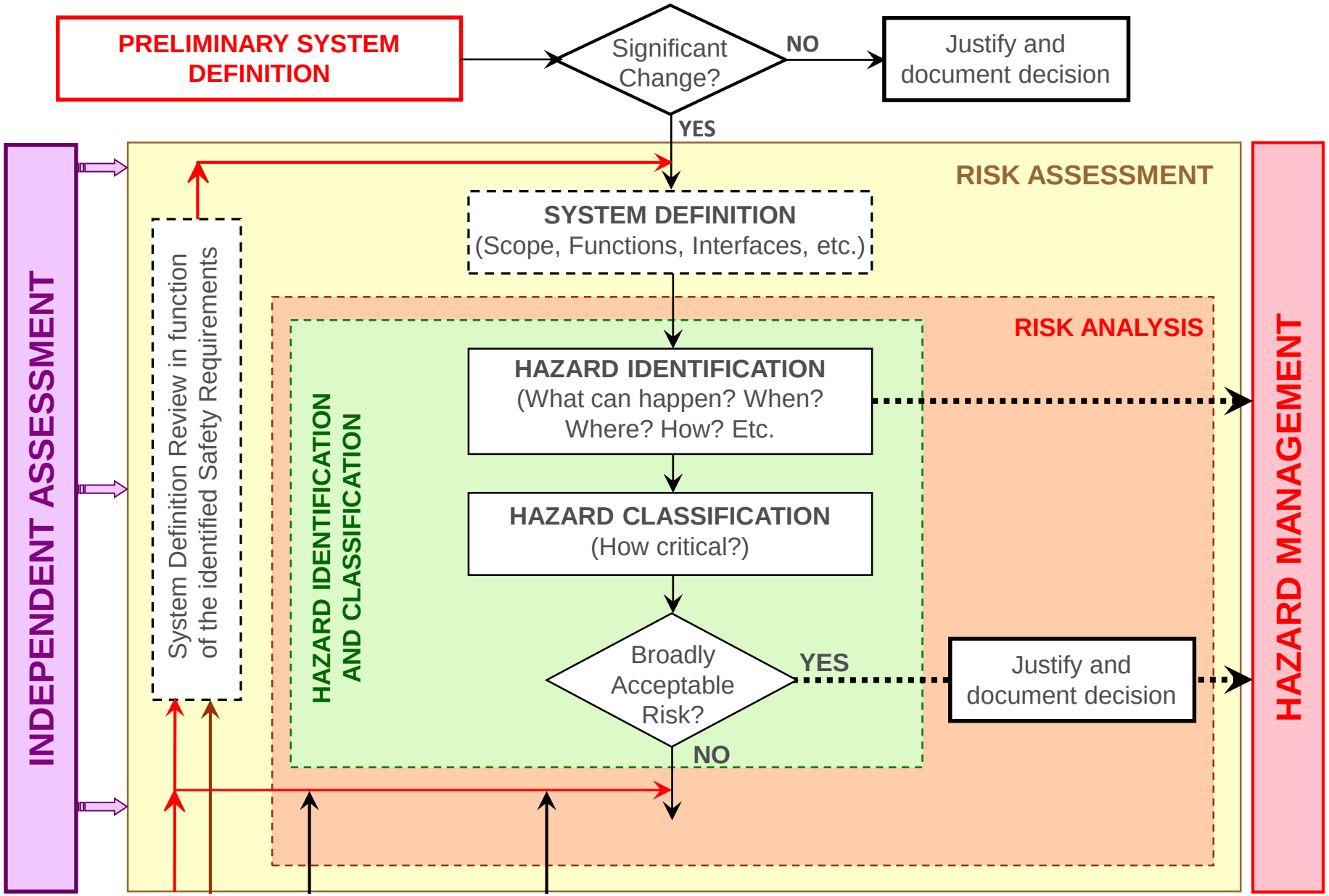
CSM, TSI, how do they relate?

- TSIs contain essential requirements related to safety only if necessary for interoperability

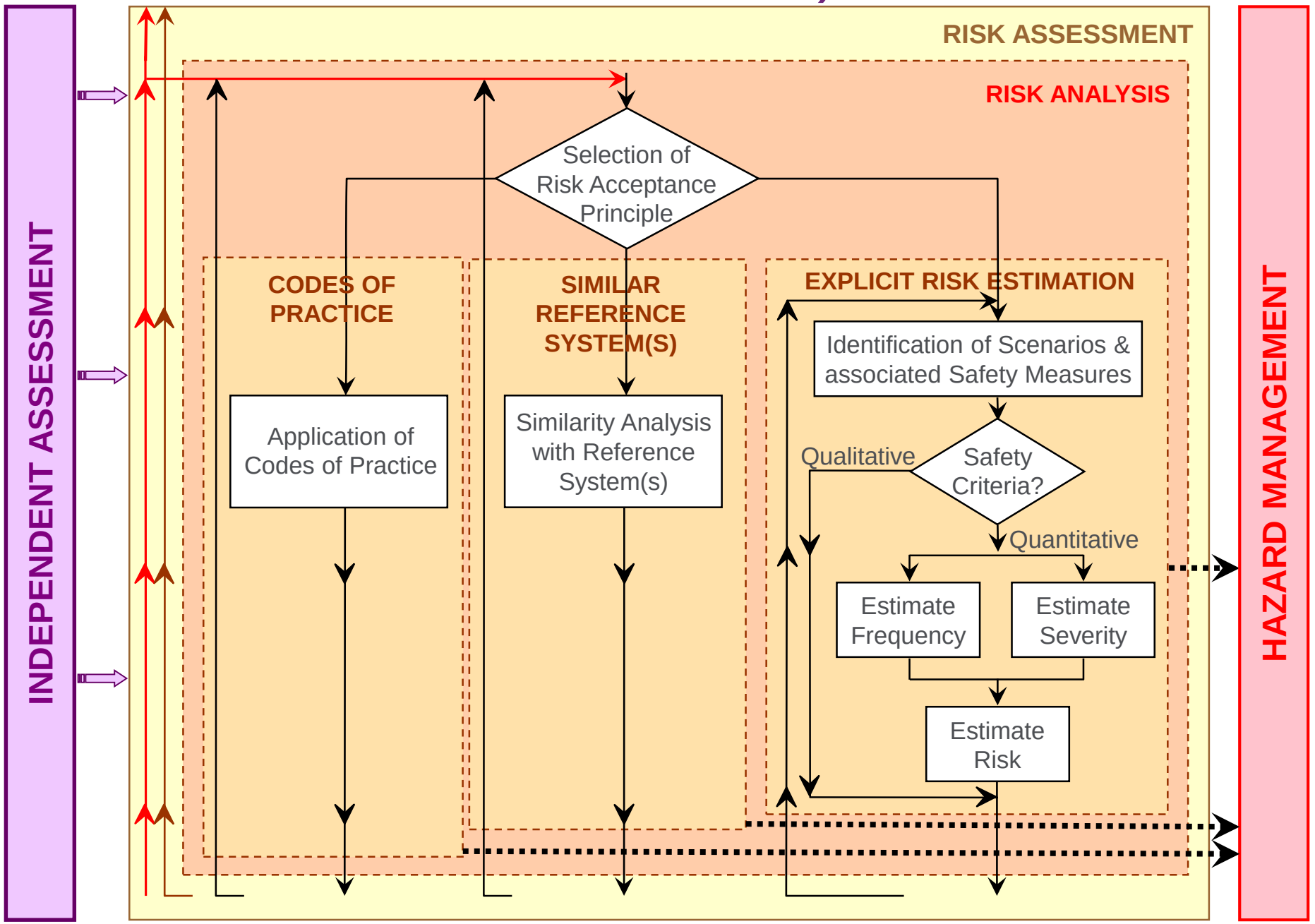
- TSIs request application of specific part(s) of CSM-RA only where necessary for interoperability

- However, sole compliance with TSIs does not ensure safety is fully covered → additional risk assessment necessary
  - → CSM-RA still mandatory for safe management of changes → **CSM RA must also be applied to demonstrate safety is fully controlled**

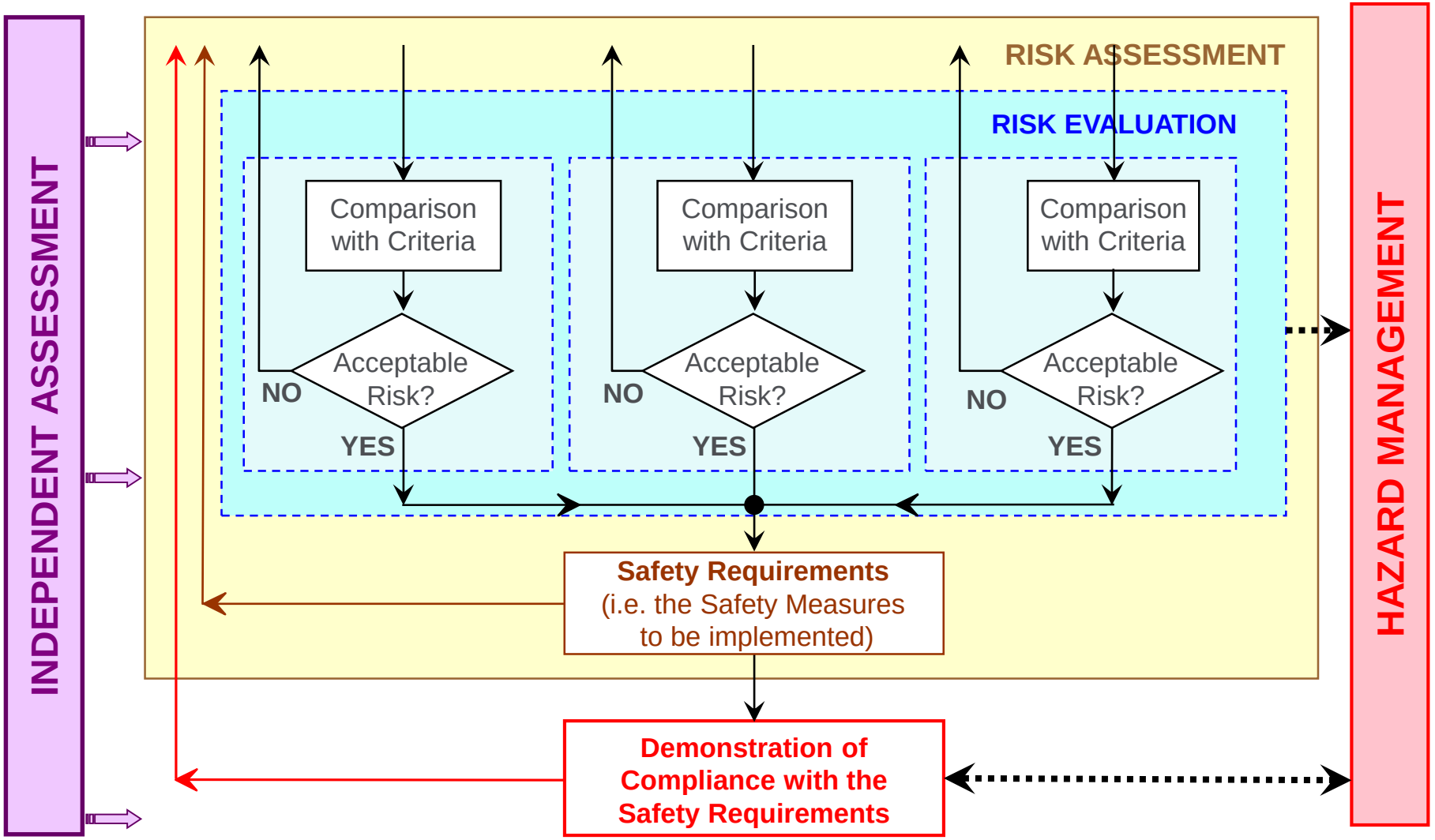
CSM-RA → what to do? → 1) Hazards



CSM-RA → what to do? → 2) RAP



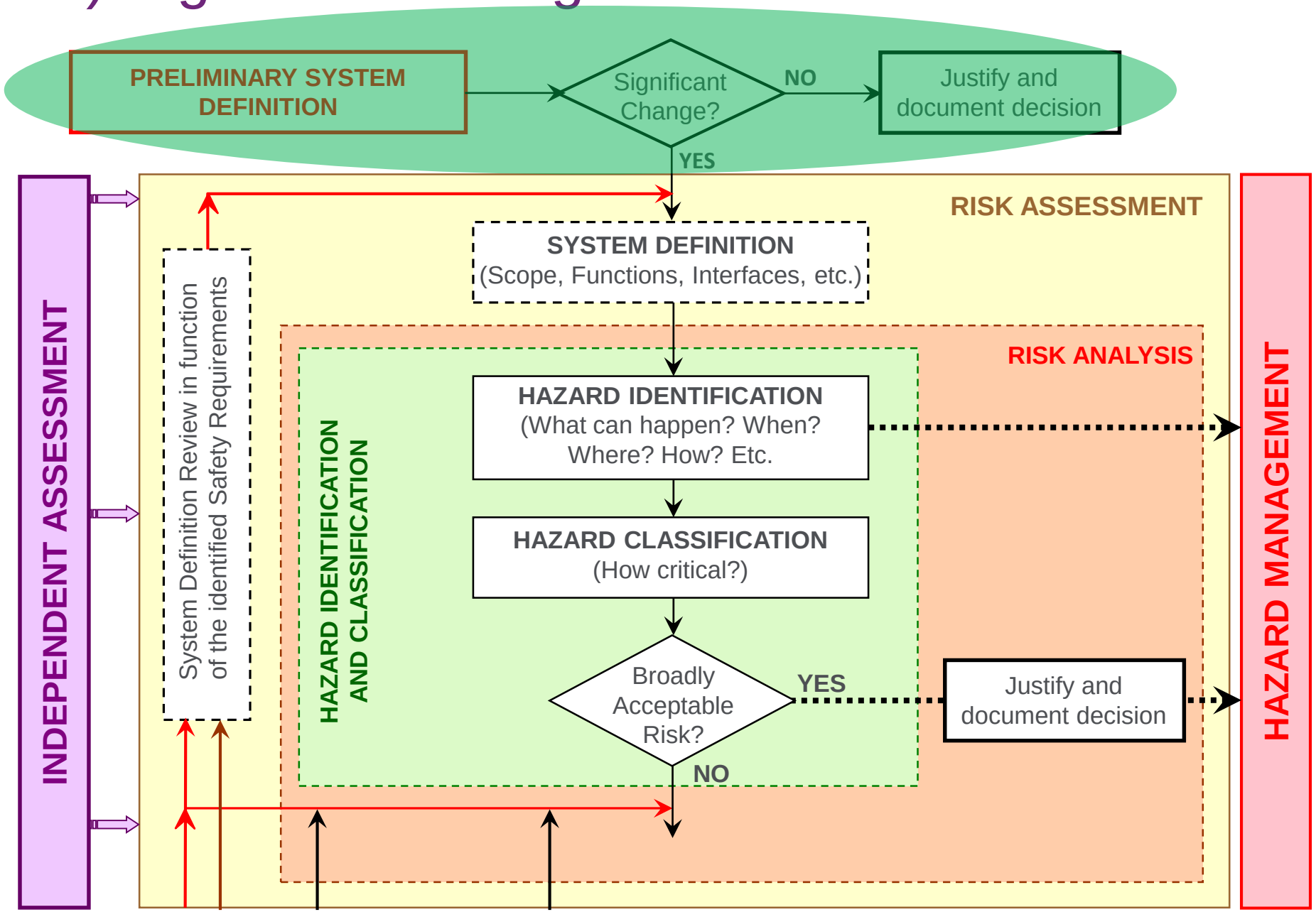
CSM-RA → what to do? → 3) Risk Evaluation & safety requirements



CSM-RA example of application

Practical examples for each step

1) Significant change?



1) Significant change? (402/2013/EU Article 4) → depends on the proposer!

- Impact on safety: if the failure of the system has the potential to lead to any injury / fatality, then there is a safety impact (as low as it may be) → application of the risk management process

- Failure consequence: credible worst-case scenario in the event of failure of the system under assessment, taking into account the existence of safety barriers outside the system under assessment
  - The failure of the system (including the potential barriers) cannot ever lead to severe injury(ies) and/or fatality(ies) → low failure consequences, probably not a significant change
  - There is a potential for severe injury(ies) and/or fatality(ies) → the other questions need to be answered, but probably a significant change

- Novelty: if the new system is totally new and unknown for the RU, then change probably significant

1) Significant change? (402/2013/EU Article 4) → depends on the proposer!

- Complexity of the change: if the change is complex (i.e. difficult to apprehend by a single person, e.g. combination of totally different competences thus different persons) then change probably significant

- Monitoring: will I be able to monitor the good behaviour of my change? Else then change probably significant

- Reversibility: am I able to reverse the modification (go back to the state before modification)? Else then change probably significant

- Additionality: taking into account the addition of this change with recent non-significant changes already put in place, would I still rank this addition as non-significant?

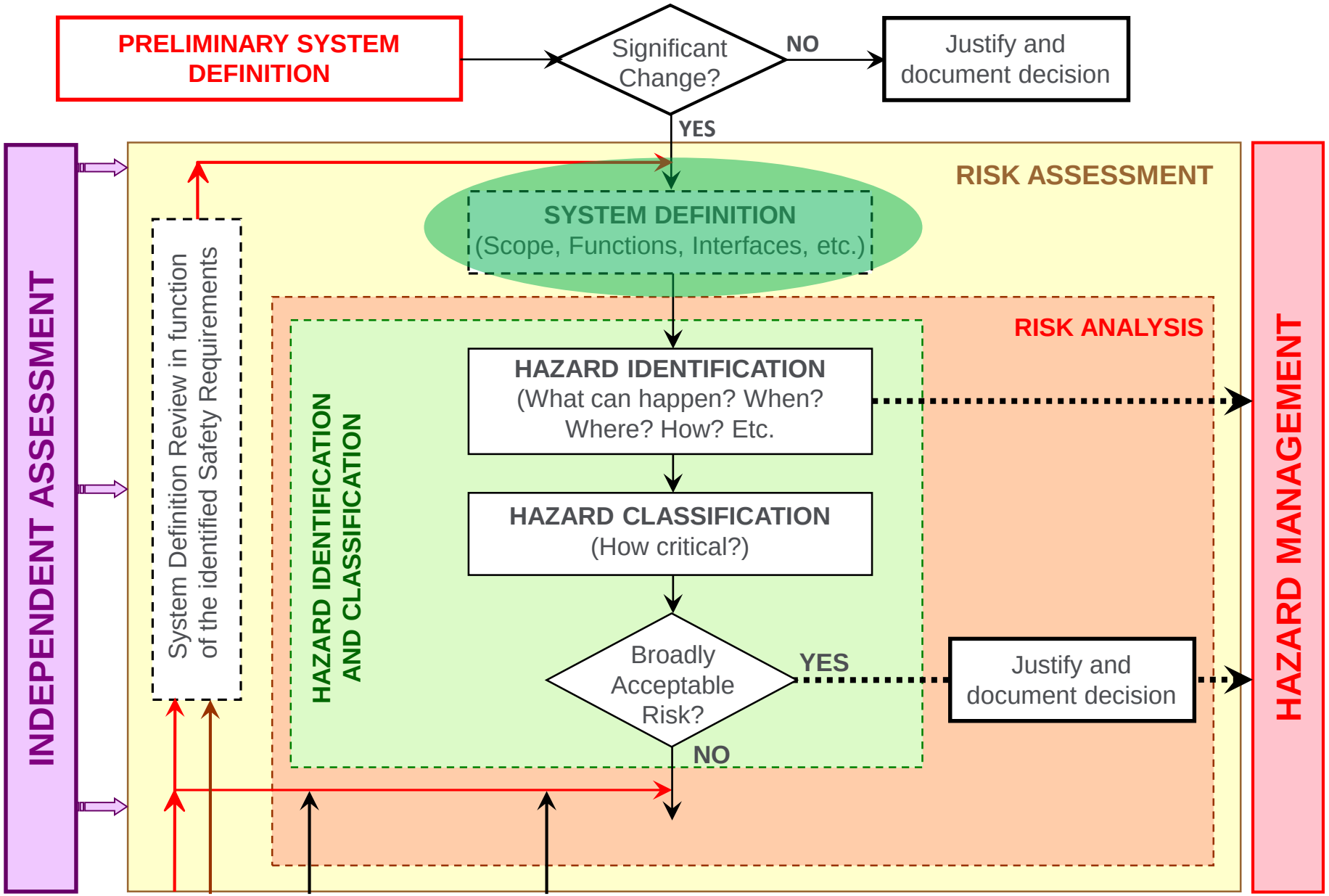
1) Significant change? (402/2013/EU Article 4) → depends on the proposer!

- Used by the proposer to differentiate modifications between the following categories:
  - No safety impact → application of CSM-RA has been completed, risk management process does not need to be applied, authorisation by NSA / EUAR is not required
  - Safety impact but change not significant → application of CSM-RA has been completed, authorisation by NSA / EUAR is not required, adequate documentation to be produced to justify the decision (the proposer should implement the change by applying its own safety method, see whereas (9) of CSM)
  - Change significant → risk management process shall be applied, NSA / EUAR authorisation may be required depending on the results of the risk management process
    - If the change does not impact the current authorisation, then no new authorisation is required
    - If the change has an impact on the current authorisation (i.e. safety demonstration requires an update with a non obvious demonstration), then an update of the authorisation (or a new one) is required

- Allows to limit the safety cases to be sent to NSA / EUAR to the relevant ones (e.g. not to changes like “replacement of the blue paint by red paint, who are both authorized paints in terms of regulation)

- Depending on the proposer’s experience (e.g. similar change already put in place), the conclusion on significance may differ from one proposer to another

2) System definition



2) System definition (402/2013/EU Annex I §2.1.2)

- Defines:
  - The change objective (why do we want that change?),
  - The system's boundary (where does the system under consideration stop?),
  - The interfaces with other systems, and with humans, e.g. Human-Machine Interface
    - List of systems, HMI, which have a link with the system under consideration
    - Content of these interfaces (what kind of link? what are the possible outputs & inputs?)
  - The system's functions (necessary for the hazard identification)
  - The system environment
    - What is the range of temperature the system is supposed to operate in? other environmental criteria? (e.g. rain, snow, …)
    - Is there electricity in the vicinity and thus possibly EMP disturbance possible?
    - Are there shocks/vibrations to which the system will be submitted?
    - How will the system be operated?
  - The safety measures already in place with the system before change (since the risk assessment process of the change may require modifications in these safety measures)
  - Assumptions that may limit the validity of the risk assessment (i.e. the aforementioned, plus other assumptions like "system used at such an emplacement", and/or "on such a train", …)

- **Without it, the risk assessment & analysis may be inadequate**

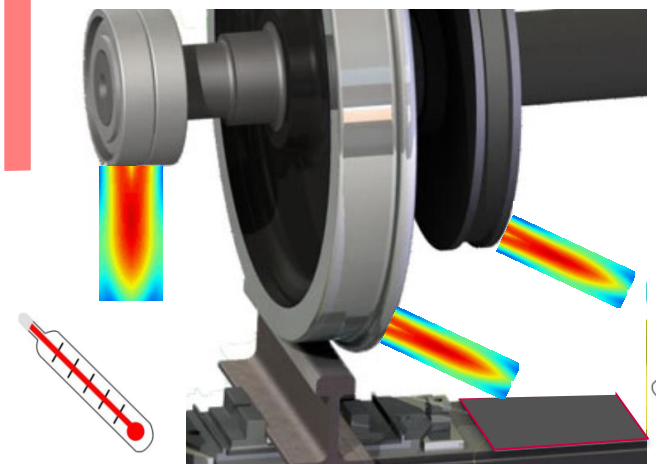
2) Example of system definition: Trainborne Hot Box Detector

Technical system under assessment

Transmit the information to the Train Driver

Detect overheating of wheelsets and axleboxes

Visual and/or audible information on overheating of a wheelset and/or an axlebox



Overheating of wheelsets and/or axleboxes

Train Driver's Cabin

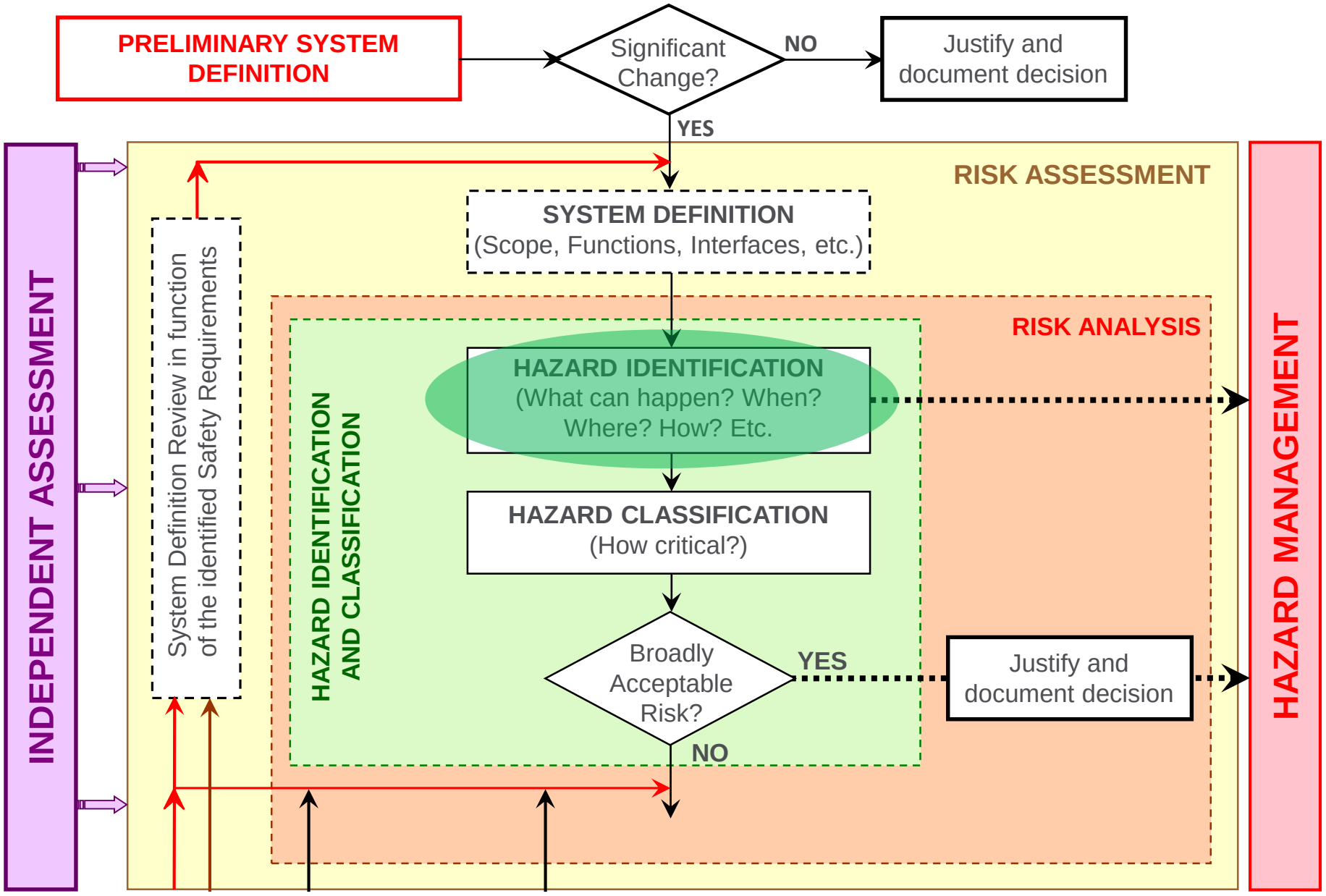
2) Example of system definition: Trainborne Hot Box Detector

- Limitations for the risk assessment (scope):
  - Statistics of hot box occurrences used are dependent on effectiveness of maintenance and operational procedures of RU SMS → may not be applicable for all trains or all RUs
  - The existing infrastructure hot box detection system is not removed and continues to be used
  - The manner those two systems are used, with any necessary operational procedures, is not covered by risk assessment below → It needs to be analyzed and evaluated in a separate risk assessment
  - Risk assessment only focusses on the technical aspects of the change
  - Failures of train driver are neither considered nor associated risk control measures proposed (the change is only on the technical system added) → It is assumed that associated human factor aspects are properly analyzed and controlled through RU SMS
  - Since hot box events can occur at any moment of time and at any location of track, operational procedures need to be defined with the Infrastructure Manager to manage:
    - Safe stopping of train at an appropriate and agreed location,
    - Reduction of speed limit for the train which suffered the hot box during the circulation up to the selected stopping location
    - Evaluation of necessity to enforce traffic stop for trains on adjacent tracks, in order to manage risks of fire due to the hot box that may spread on trains circulating in the adjacent tracks

2) System definition → what if it is not done?

- The safety studies might be invalid (e.g. limitation of the safety study incompatible with the foreseen operation of the system), thus
  - Potentially missing unidentified risks → risk of casualties
  - Underestimating some risks → risk of casualties
  - Overestimating some risks → unnecessary expenses
  - Change not authorized by NSA (or safety certificate challenged if discovered during audit) → delays & costs
- Some interfaces may be forgotten, thus
  - Potentially missing unidentified risks → risk of casualties
  - Underestimating some risks → risk of casualties
  - Overestimating some risks → unnecessary expenses
  - Change not authorized by NSA (or safety certificate challenged if discovered during audit) → delays & costs
- Examples:
  - The link between the Trainborne Hot Box Detector and the driver is forgotten → the driver is not alarmed by the system in case of hot box detection → the system is useless
  - The safety study is considered applicable if the On-track Hot Box Detectors are still in place, but this is not the case → the safety is solely on the On-board system, which no longer has a sufficient safety level → risk of casualties

3) Hazard identification



3) Hazard identification (402/2013/EU Annex I §2.2)

- Requires the identification of all reasonably foreseeable hazards
  - Means: if my system fails, what are the potential accidents that can occur (generally at the train operation level, but also potentially for the user in case of fire, explosion, …)
  - Ensure of course that normal operation (without failure) cannot lead to injury(ies) / casualty(ies) (else, specific operation procedure will be necessary to cover those risks)
  - You are not expected to take into account meteors, nuclear explosions, … → if the accident studied will be exactly the same whether your system is here or not, and touches in exactly the same way people which are totally outside (and far apart) of the railway, then this accident is probably out of scope
- Typically carried out through a functional approach (at least for complex systems)
- Generally checked with a list of known classic hazards (experience of the company + standardized lists for the domain) to cover potential misses
- **Without it, the risk assessment & analysis may be inadequate/incomplete**

3) Example of Hazard identification: Trainborne Hot Box Detector → functional FMEA

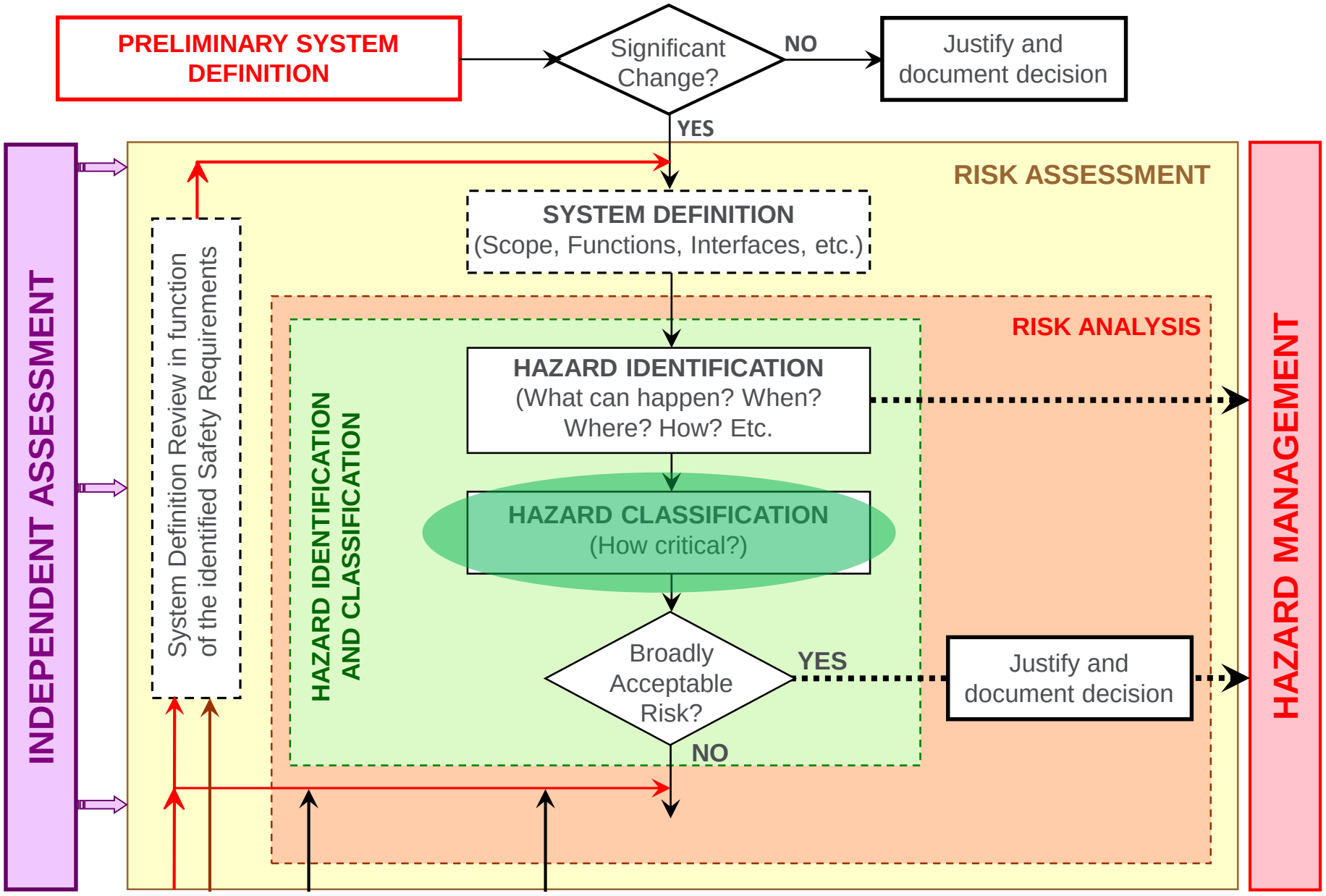
N°	Function	Functional failure modes	Cause	HAZARD - Consequence at level of technical system	Consequences at train level
1.	Trainborne Hot Box Detection	Detection does not start	• Hot Box Detector failed • Failure of indication system	Hot Box Event not detected by technical system when required	In case of a Hot Box Event, the driver is not informed and cannot stop the train safely.
2.		Detection starts when not required	• Hot Box Detector failed • Failure of indication system	Spurious detection of a Hot Box Event	• Driver required to stop the train whereas not necessary • Traffic operation disturbed
3.		Detection does not stop when required	• Hot Box Detector failed • Failure of indication system	Spurious detection of a Hot Box Event	• Driver required to stop the train whereas not necessary • Traffic operation disturbed
4.		Detection stops when not required	• Hot Box Detector failed • Failure of indication system	Hot Box Event not detected any more by technical system whereas still required	In case of a Hot Box Event, the driver can be misled (e.g. believes it is a false alarm) and could ignore the alarm whereas he shall stop the train safely.
5.		Detection is delayed in response	• Hot Box Detector failed • Failure of indication system	Hot Box Event may not be detected on time to permit actions to be put in place to ensure the safety	In case of a Hot Box Event, the driver is informed too late and might not stop the train safely.
6.		Detection degraded (e.g. wrong output level)		Not applicable. The hot box detection is a binary output	Not applicable. The hot box detection is a binary output

3) Hazard identification → what if it is not done?

- Hazards may not be studied
  - Potentially missing unidentified risks → risk of casualties
  - Non-safety major impacts may be ignored → design not useable / not satisfying in operation → cost of redesign
  - Change not authorized by NSA (or safety certificate challenged if discovered during audit) → delays & costs

- Examples:
  - The system has a perfect safety, but continuously impedes operation → the system is isolated, thus the railway is less safe than before the system was introduced!
  - New technology of electromagnetic levitation instead of wheels → risk of magnetic interferences to pacemakers → risk of casualties

4) Hazard classification



4) Hazard classification (402/2013/EU Annex I §2.2)

- Requires the classification of all identified hazards
  - Using the identified potential consequences at train level during hazard identification
  - Using the severity classes defined in the Common Safety Method:
- 1st filter: all failures which do not have a safety impact → application of the risk management process is not required by the authorisation process
- 2nd filter: failures which do not have the potential for at least 1 fatality → possibility of “broadly acceptable” (see step 5.)
- 3rd filter: consequence limited to a specific area of the train → allow for the severity category choice (and thus the CSM-DT category, see 2015/1136/EU)
- Generally checked with a list of known classic hazards (experience of the company + standardized lists for the domain) to cover potential misses
- **Without it, the risk assessment & analysis may be inadequate/incomplete**

4) Example of Hazard classification: Trainborne Hot Box Detector → continuation of functional FMEA

CSM-DT → 10^{-9} / h

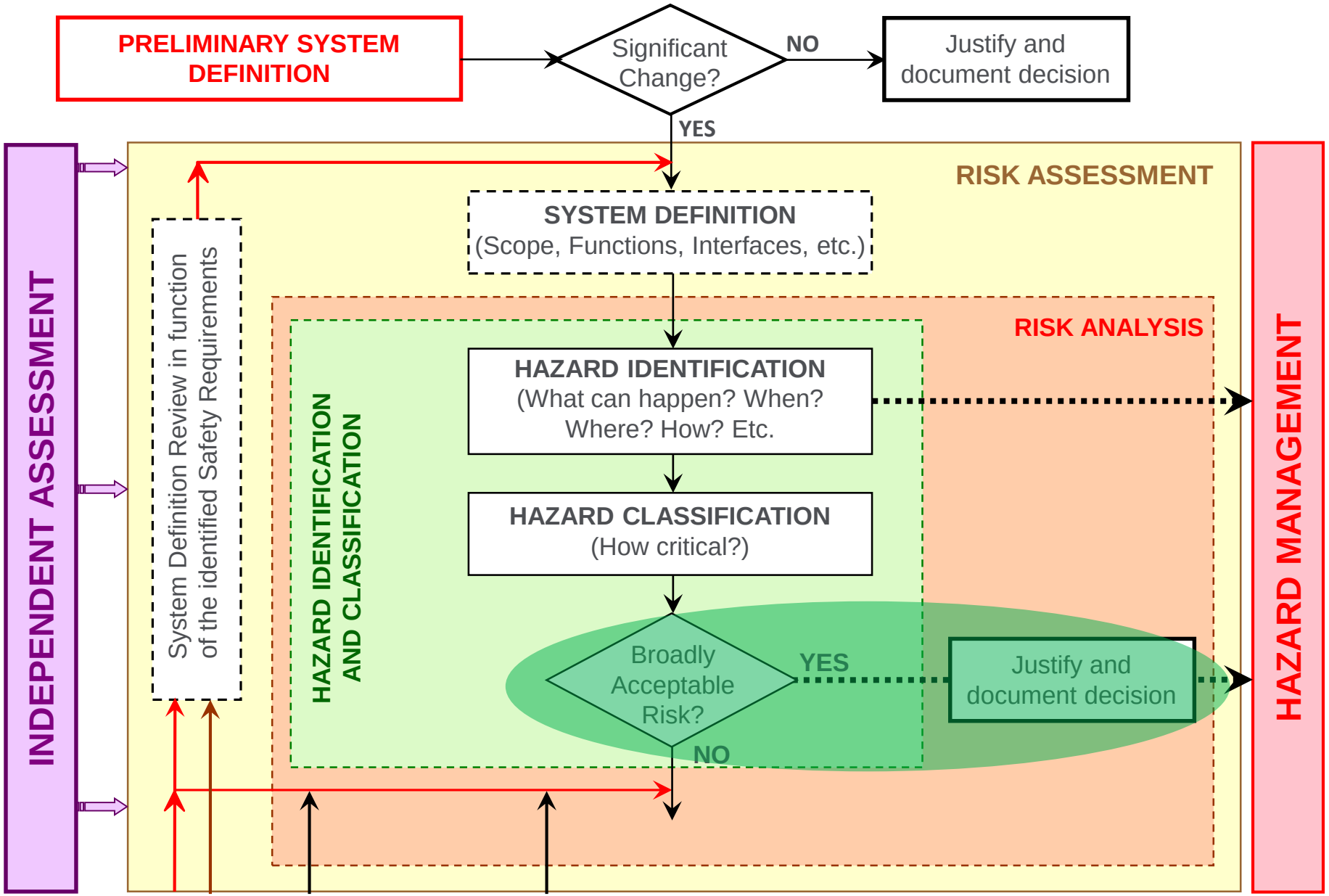
N°	...	HAZARD - Consequence at level of technical system	Consequences at train level	Potential accident	Potential for at least 1 fatality	Consequence limited to a specific area of train
1.		Hot Box Event not detected by technical system when required	In case of a Hot Box Event, the driver is not informed and cannot stop the train safely.	• Fire • Derailment	YES (i.e. risk not broadly acceptable)	NO (whole train exposed to risk)
2.		Spurious detection of a Hot Box Event	• Driver required to stop the train whereas not necessary • Traffic operation disturbed	No – Specific operational procedures must be defined to prescribe the actions of the driver when a Hot Box Detector reports a false alarm	No safety impact	
3.		Spurious detection of a Hot Box Event	• Driver required to stop the train whereas not necessary • Traffic operation disturbed			
4.		Hot Box Event not detected any more by technical system whereas still required	In case of a Hot Box Event, the driver can be misled (e.g. believes it is a false alarm) and could ignore the alarm whereas he shall stop the train safely.	• Fire • Derailment	YES (i.e. risk not broadly acceptable)	NO (whole train exposed to risk)
5.		Hot Box Event may not be detected on time to permit actions to be put in place to ensure the safety	In case of a Hot Box Event, the driver is informed too late and might not stop the train safely.	• Fire • Derailment	YES (i.e. risk not broadly acceptable)	NO (whole train exposed to risk)
6.		Not applicable. The hot box detection is a binary output	Not applicable. The hot box detection is a binary output	Not applicable		

4) Hazard classification → what if it is not done?

- Design may not be in accordance with safety
  - Potentially underestimated risk → risk of casualties
  - If current design not safe enough → design not useable → cost of redesign
  - Change not authorized by NSA (or safety certificate challenged if discovered during audit) → delays & costs

- Examples:
  - An on-the-shelf system exists on the market, which is SIL2, which fulfils the required function. However, a SIL2 system is not able to achieve alone a safety requirement of 10^{-9} / h (potential for multiple fatalities, not limited to a specific area of the train)
  - Depending on the scope of the modification (see step 1.), the hazards potential consequence may differ:
    - Braking distance augmented by 10% on a heavy traffic line → collision possible → risk of casualties
    - Braking distance augmented by 10% on a line where no other train circulate → no risk of collision → potentially no safety impact? (except if collision possible with infrastructure?)

5) Broadly acceptable risk?



5) Broadly acceptable risk? (402/2013/EU Annex I §2.2)

- Allows for limiting the safety study to risk which really require an analysis
- An estimation on the frequency of the hazard is made (generally through an expert judgment)
- Combination of Frequency and Severity (potential consequences) → Risk = F x S
  - If frequency very rare AND severity low (e.g. no potential for fatality, but still potential for light injury(ies)), then probably broadly acceptable (no clear rule on a threshold)
  - If frequency not rare OR severity no low (e.g. potential for fatality and/or frequent failures of this system), then not broadly acceptable → acceptance of the risk needs to be demonstrate through the application of a Risk Acceptance Principle (see step 6.)
- **Be careful to have a coherent judgement on "Broadly acceptable" among the different projects, and to define a threshold (or a process on how to make that judgement)**

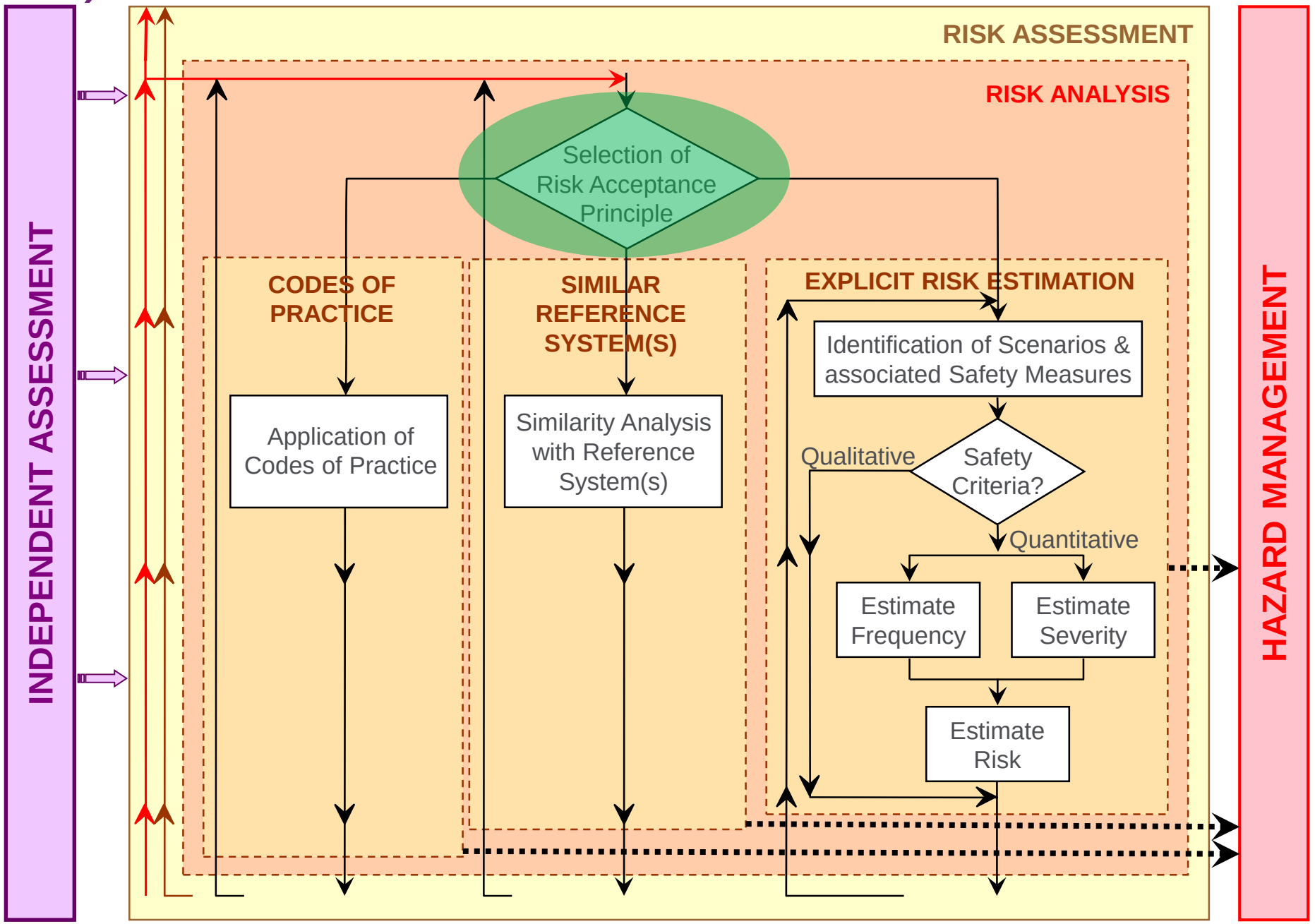
5) Example of Broadly acceptable risk: Trainborne Hot Box Detector

- Since the identified hazards have been considered as having potential consequences of at least one fatality, and not limited to a specific area of the train, the risk cannot be considered as broadly acceptable (proofs need to be assessed that the risk can be considered as acceptable → see step 7.)

5) Broadly acceptable risk → what if it is not done?

- Safety is not hindered, only unnecessary safety study
- **Be careful however not to have judge too easily that a risk is broadly acceptable (e.g. no clear rule) as an NSA audit may endanger the safety certificate**

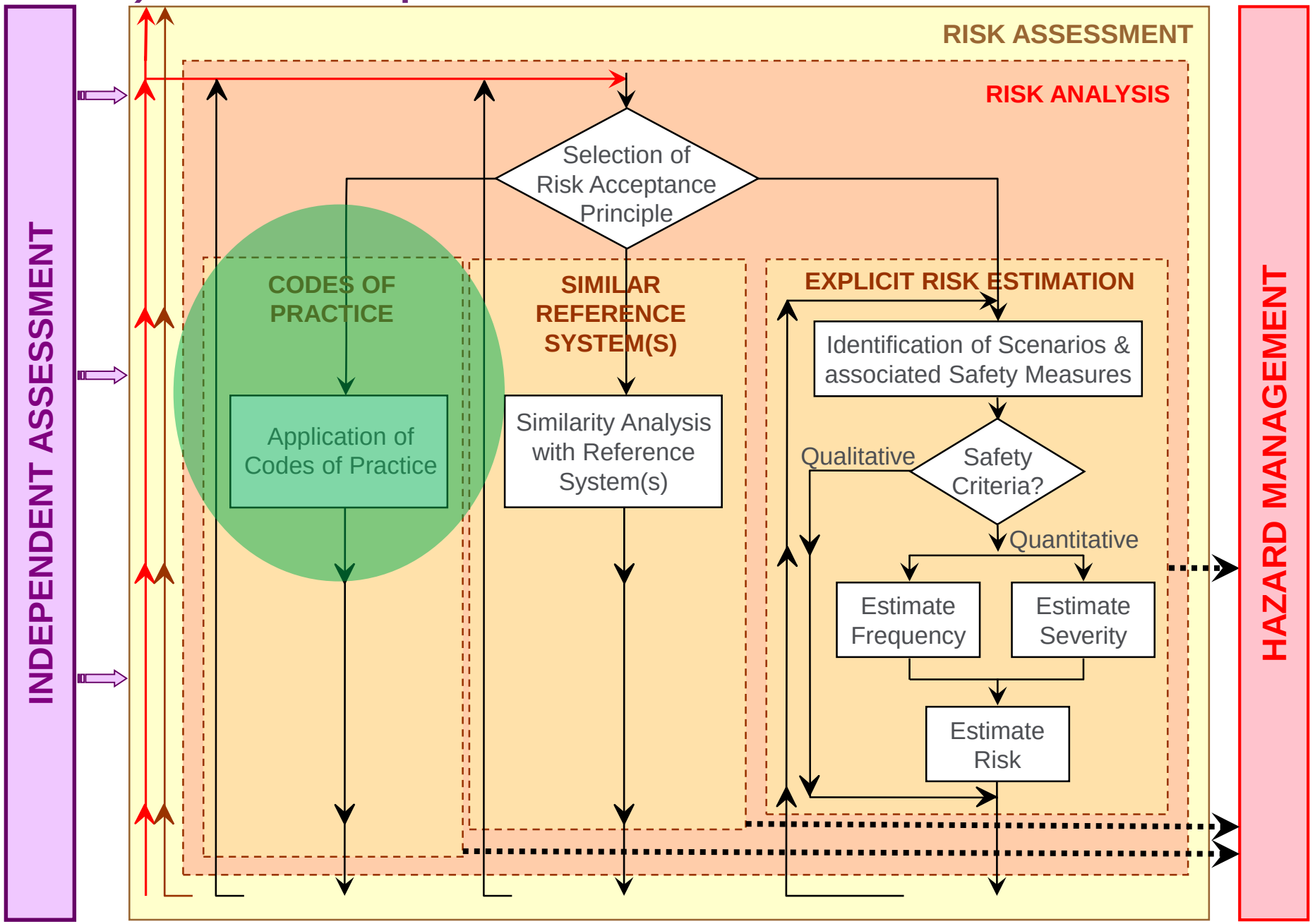
6) How to select the RAP?



6) How to select the RAP? (402/2013/EU Annex I §2.1.4 to 2.1.6)

- The choice of the Risk Acceptance Principle(s) equals to the strategy you intend to use to demonstrate that the change is safe
- Application of a Code of Practice, which states what to do (e.g. application of a UIC leaflet, of a EN standard, …)
  - Proof of correct application of the CoP is considered as sufficient
  - However, depending on the CoP, mutual recognition is not assured (i.e. is this CoP also considered sufficient in the other country → to be discussed with the NSA in the early project)
- Comparison of the change to a similar change made in the past and which has been (and would still be) authorized
  - The change will be accepted if the achieved safety is at least as good as for the other change
  - However, the change taken as a reference may not be applicable to all countries (e.g. this train is not authorized in this country) → mutual recognition is not assured
- Explicit Risk Estimation, to evaluate whether the risk is acceptable
  - Either qualitatively through use of tables (e.g. I am in case A3, which is acceptable, B7 would not be)
  - Or quantitatively through probabilistic studies
  - As long as the safety study's limitations are applicable in the other country, mutual recognition is assured

7.a) Code of practice



7.a) Code of practice (402/2013/EU Annex I §2.3)

- To be considered valid, a CoP must be:
  - widely recognized in the railway domain. If this is not the case, the codes of practice will have to be justified and be acceptable to the assessment body
  - relevant for the control of the considered hazards in the system under assessment → successful application of a code of practice for similar cases to manage changes and control effectively the identified hazards of a system in the sense of this Regulation is sufficient for it to be considered as relevant
  - available upon request to assessment bodies for them to either assess (or where relevant mutually recognize) the suitability of both the application of the risk management process and of its results

- Note that a CoP may require Explicit Risk Estimation (e.g. TSI Loc & Pas) on some subjects

- Typical CoPs are (to be validated by each NSA):
  - UIC leaflet
  - TSIs
  - Harmonised standards: e.g. http://ec.europa.eu/growth/single-market/european-standards/harmonised-standards/
  - Internal process/rules (but no mutual recognition)

7.a) Example of Code of practice: Trainborne Hot Box Detector

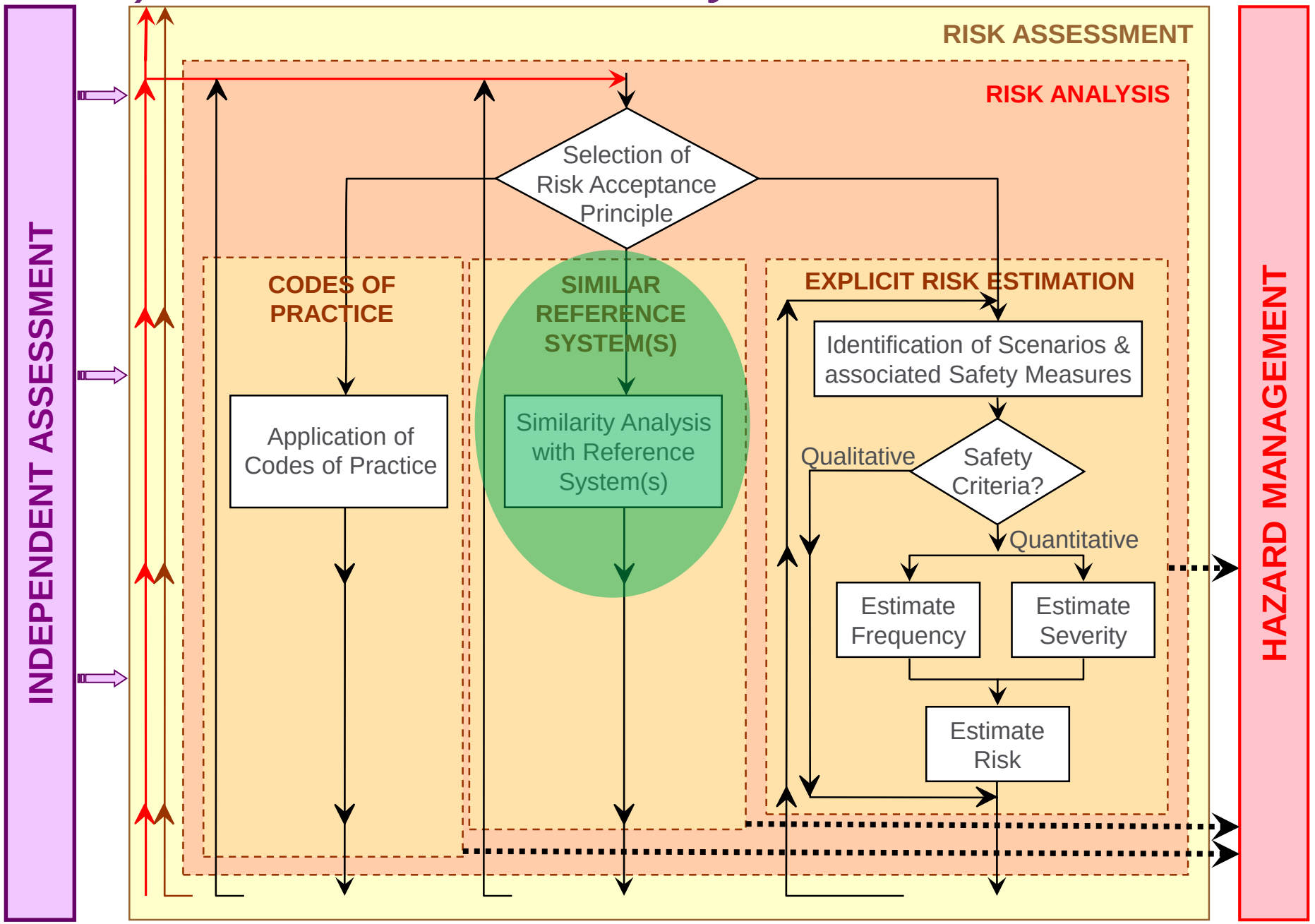
- TSI Loc&Pas § 4.2.3.3.2 (high level requirements only)
- EN 15437-1:2009 (especially § 5.1 & 5.2) → rather for on-track detectors

Thus code of practice does not appear to be able to cover completely the acceptance (no recognized CoP for on-board detectors)

7.a) Code of practice: what if used incorrectly / not used?

- Application of CoP which does not cover sufficiently the hazard(s) → change not authorized by NSA (or safety certificate challenged if discovered during audit) → delays & costs
- Non application of an applicable CoP → risk of unnecessary cost / delay
- Be careful though: systematic application of CoP hinders innovation!

7.b) Similar Reference System



7.b) Similar Reference System (402/2013/EU Annex I §2.4)

- To be considered a valid reference, a system must:
  - have already been proven in-use to have an acceptable safety level and would still qualify for approval *in the Member State* where the change is to be introduced
  - have similar functions and interfaces as the system under assessment
  - be used under similar operational conditions as the system under assessment
  - be used under similar environmental conditions as the system under assessment

- A similar reference system analysis may be carried through:
  - Use of the exact same solution (schematics and characteristics are identical)
  - Qualitative statement on obvious enhancement of safety (e.g. same schematic, but adding a redundancy)
  - Explicit Risk Estimation (e.g. fault tree to demonstrate that the safety level reached by the system under assessment is at least as safe than the one reached by the reference system)

7.b) Example of Similar Reference System: Trainborne Hot Box Detector

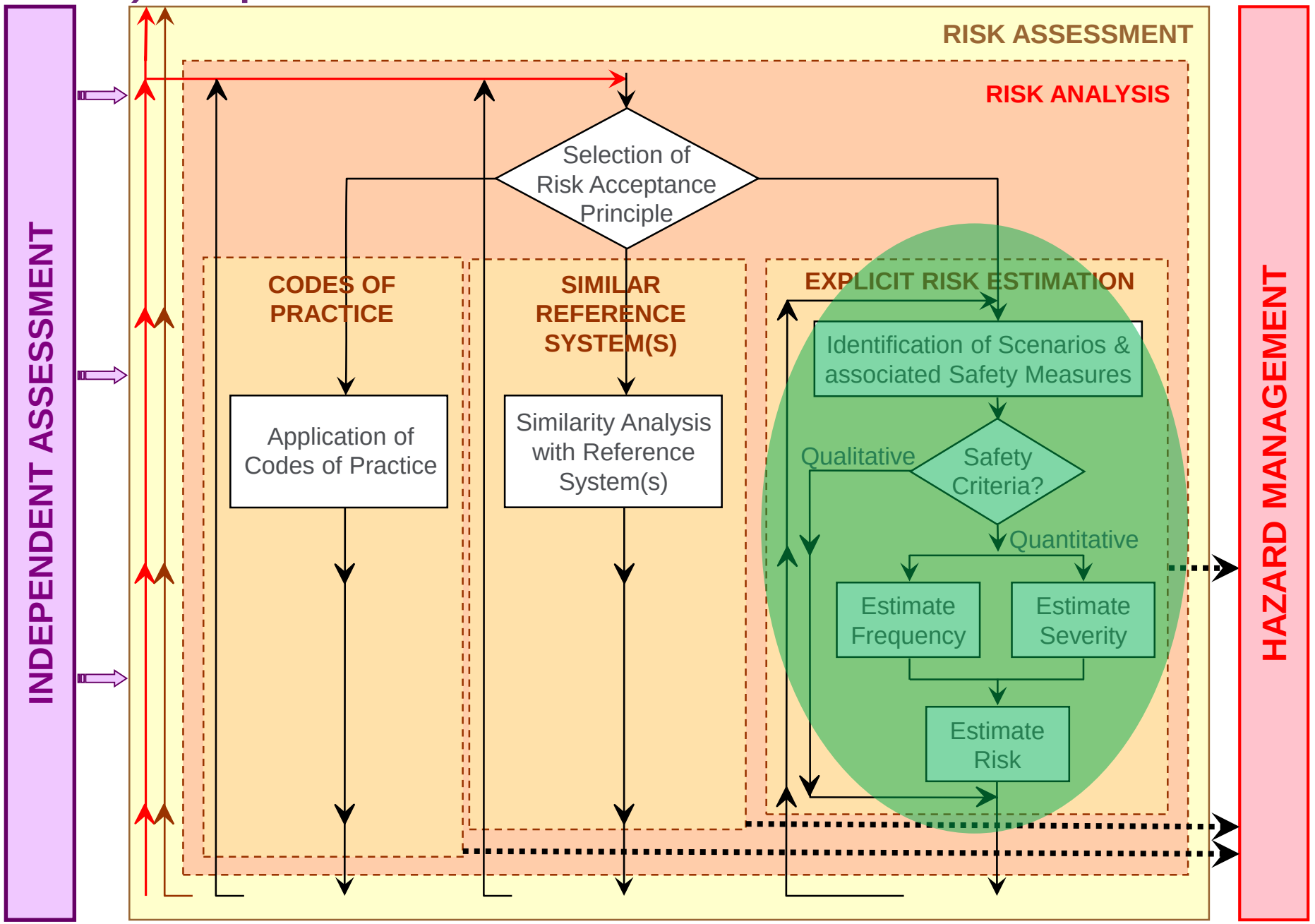
- Comparison with on-track detectors
  - but a detector on the track every X m → if a hot box is not detected by one, the following should
  - If on-board detector(s) of a specific wheel box fail, then a hot box will never be detected!

Feasible, but will not be simple, and depending on the network/country, the study may no longer be applicable (e.g. distance between on-track detectors different than in my country)

7.b) Similar Reference System: what if used incorrectly / not used?

- "Reference System" which does is not valid to be taken as a reference → change not authorized by NSA → delays & costs
- Non application of an applicable Similar Reference System → risk of unnecessary cost / delay

7.c) Explicit Risk Estimation



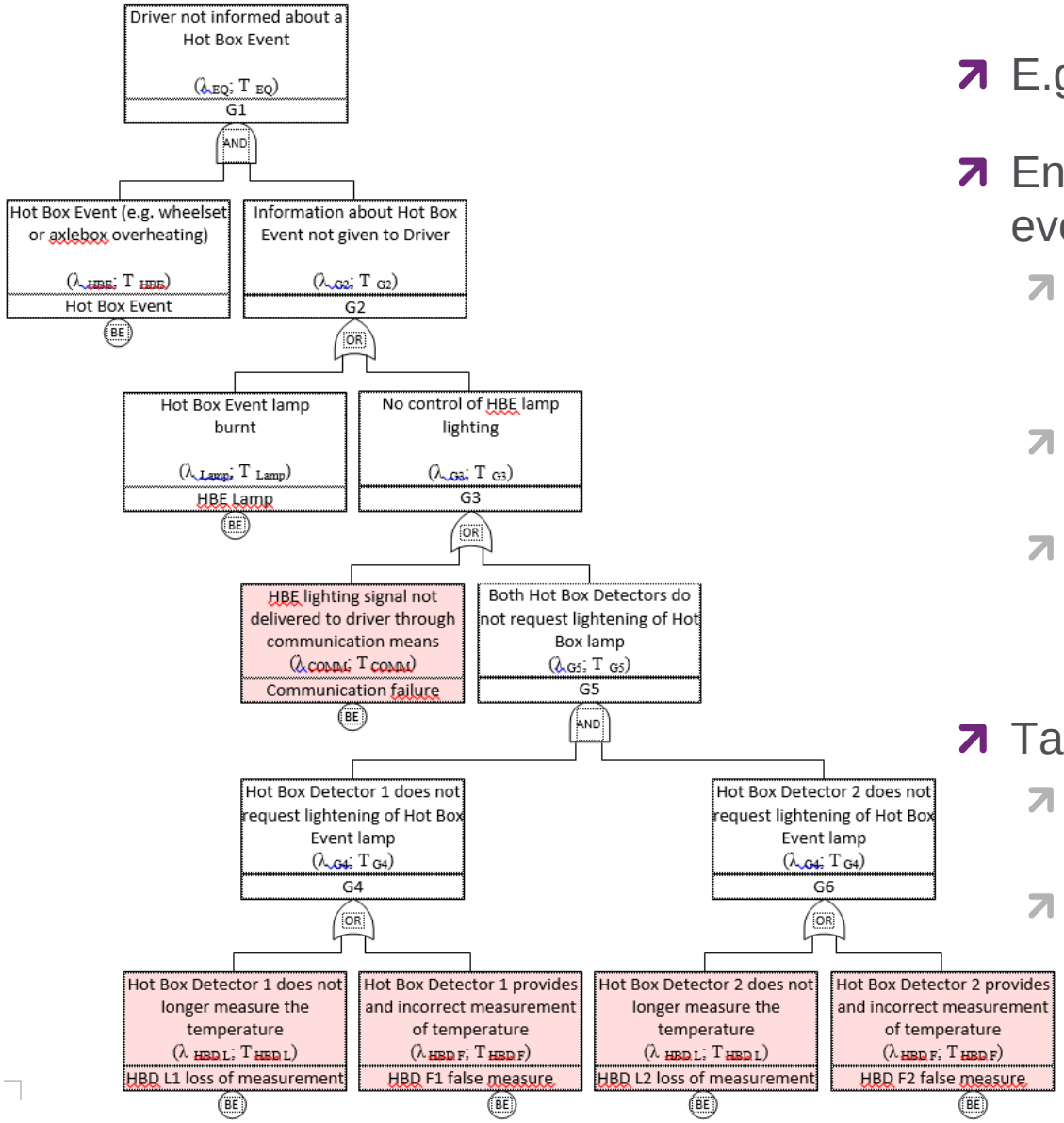
7.c) Explicit Risk Estimation (402/2013/EU Annex I §2.5)

- Quantitative and/or qualitative approach
  - Quantitative → probabilistic study (e.g. fault tree)
  - Qualitative → rather semi-quantitative, use of defined categories (e.g. risk matrix, Safety Integrity Level, number of failures required, …)

- Quantification → Common Safety Method-Design Targets
  - Where a failure has a credible potential to lead directly to a catastrophic accident, the associated risk does not have to be reduced further if the frequency of the failure of the function has been demonstrated to be highly improbable → 10^{-9} / h (see definition (35) of catastrophic accident of 2015/1136/EU)
  - Where a failure has a credible potential to lead directly to a critical accident, the associated risk does not have to be reduced further if the frequency of the failure of the function has been demonstrated to be improbable → 10^{-7} / h (see definition (36) of critical accident of 2015/1136/EU)
  - The choice between definition (23) and definition (35) shall result from the most credible unsafe consequence of the failure

- See Guide on harmonized design targets (CSM DT)

7.c) Example of Explicit Risk Estimation: Trainborne Hot Box Detector

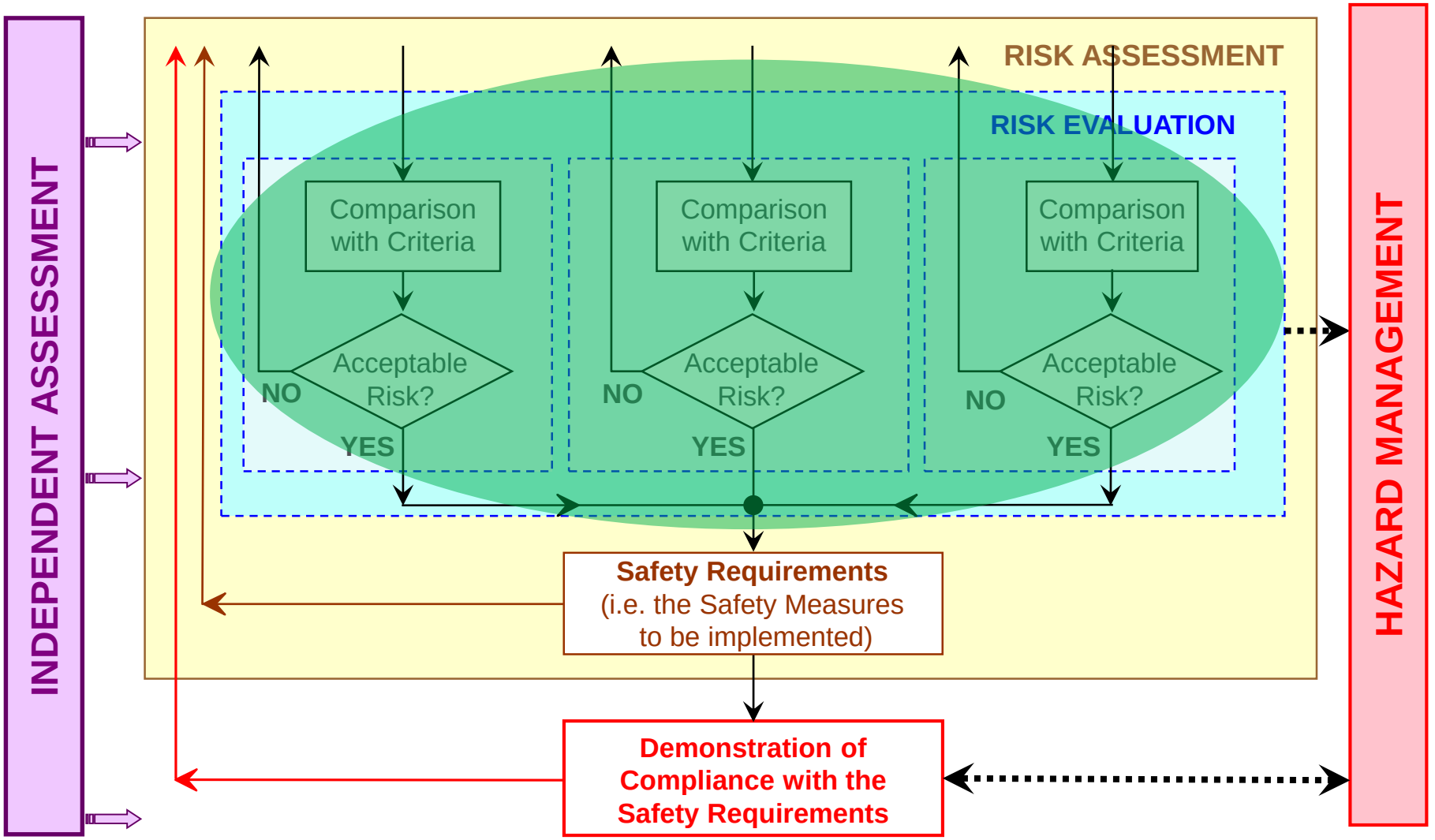


- E.g. fault tree analysis
- Ensure independence between events, i.e.:
  - The hot box does not immediately trigger a failure of the detector(s)
  - The detector's failure does not trigger a hot box
  - A detector's failure does not trigger the failure of the other detector
- Take into account maintenance:
  - When at the latest be a failure be detected?
  - When at the latest will it be repaired?

7.c) Explicit Risk Estimation: what if used incorrectly / not used?

- Independence not verified → a failure will trigger another failure, thus the safety target is not reached → system no accepted by NSA, redesign necessary → costs & delays
- Failure rates / probabilities for component's failure not realistic → number of accidents higher than expected → risk of losing the authorisation for the system (the train)
- Safety study built on the functional description rather than on the schematics → wrong results → number of accidents higher than expected → risk of losing the authorisation for the system (the train)
- Non application of Explicit Risk Estimation → risk of no mutual recognition of the study

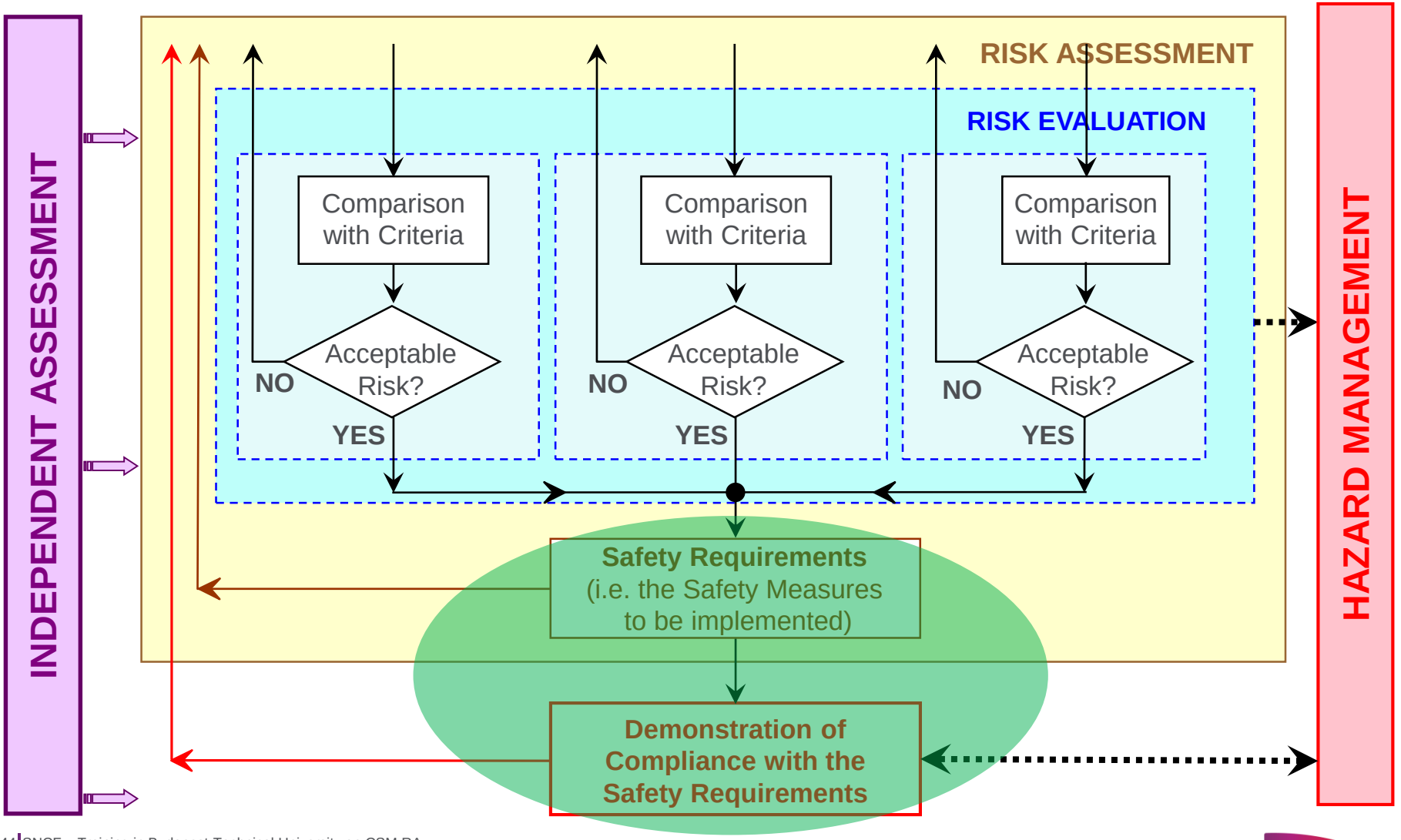
8) Risk evaluation



8) Risk Evaluation

- Verification by the proposer (and the CSM Risk Assessment Body) that the criterion/criteria chosen through the Risk Acceptance Principle is/are met, i.e.:
  - For a Code of Practice: assurance that the requirements of the CoP are met, that the CoP has been correctly applied (see 402/2013/EU Annex I §2.3.5 to 2.3.8)
  - For a Similar Reference System: assurance that the system is at least as safe than the reference system. In case of deviation from the reference system where a lower safety is reached, then additional safety measures shall be identified to ensure a sufficient overall safety (see 402/2013/EU Annex I §2.4.3 to 2.4.5)
  - For an Explicit Risk Estimation:
    - Qualitative: ensure that the qualitative criterion/criteria is/are met (e.g. correct SIL, the estimated risk remains in the acceptable zone, …)
    - Quantitative: ensure that the CSM-DT are reached
    - See 402/2013/EU Annex I §2.5.3 to 2.5.12

9) Safety Requirements (e.g. operational & maintenance constraints)



9) Safety Requirements (e.g. operational & maintenance constraints)

- Demonstration by the proposer that the safety requirements identified through the risk analysis are met, i.e.:

  - Maintenance requirements are coherent with maintenance strategy in place (or its update) → e.g.:
    - This component is verified in maintenance every month
    - This component's failure (once detected) will be repaired at the latest 1 week later

  - Operational requirements are present in the operational procedures → e.g.:
    - Tests to be carried out at the start of the train
    - List of failures which forbid the use of the train
    - List of failures where the operation is possible but with restriction (e.g. only for the current day then repair, speed restriction, system's isolation, …)

  - Specific formation to put in place for some categories of personnel

  - …

9) Example of Safety Requirements (e.g. operational & maintenance constraints): Trainborne Hot Box Detector

- Exported constraints on the infrastructure:
  - Ensure presence of on-track detectors every X meters (more important distance is allowed if all trains on this line are equipped with trainborne detectors, and/or their reliability may be relaxed depending on the safety level reached by the on-board detectors)
  - Ensure presence of on-track detectors as long as trains without trainborne detectors may operate on this line
- Exported constraints on the maintenance:
  - Test the trainborne detectors' efficiency regularly (e.g. each month?)
  - When a detector's failure is known, the train cannot leave the maintenance center before the detector has been repaired/replaced → maintenance procedure, formation of maintenance personnel
- Exported constraints on the rolling-stock (operational procedure, formation of drivers):
  - Ensure that the driver is immediately notified of a detected hot box (typically sound + lamp)
  - Ensure that the driver is notified of a detector's failure (kind of alarm? immediate or at stop?)
- Exported constraints on the operation:
  - When a detector's failure is notified, indicate restrictions (e.g. speed restriction? Limited time of operation?)
  - When a hot box is notified, indicate restrictions (e.g. speed restriction? Limited time of operation?)

9) Safety Requirements (e.g. operational & maintenance constraints): what if it is not done

- Possibility of unsafe uses of the train (e.g. circulating with a reduced capacity of braking without speed restriction → collision)

- Possibility of invisible degradation of safety performance (e.g. no visible failure due to redundancy, but next failure will trigger the accident)

- Misuses of the system (personnel not formed → isolation of the system without putting in place the restrictions, filling of incorrect inputs, …)

Detected by NSA audit → risk of losing train authorisation, or worse, safety certificate

Conclusion

Is CSM-RA totally new work?

Conclusion

- Formalization of hazard analysis (necessary for new systems / new technologies)
  - Not always done in the past, as proven systems? → if no innovation, then you are capable to provide the hazards
  - Generally provided by the supplier, but need of the Railway Undertaking for its knowledge of operation (i.e. what are the potential consequences of this failure on my network?)
- Introduction of Risk Acceptance Principles:
  - Codes of Practice & Similar Reference for “keep working as we do”, but mutual recognition not assured
  - Explicit Risk Estimation to have undisputable common ground for mutual recognition
- Traceability of safety requirement to ensure that they are put in place (e.g. speed limit in case of failure detection, access denied on certain lines, …)
- Independent assessment to provide good confidence on the results of safety studies (and thus facilitate mutual recognition & interoperability)

Thus: few real novelties, rather harmonization to help interoperability