PARIS
2 ▸ 7
OCTOBER
2016 ▸ Pullman Bercy Hotel

INTERNATIONAL
RAILWAY SAFETY COUNCIL

A SAFETY ALLOCATION METHODOLOGY FOR A NEW TRAIN DEVELOPMENT

Philippe COZZARIN, Rolling Stock Safety Expert

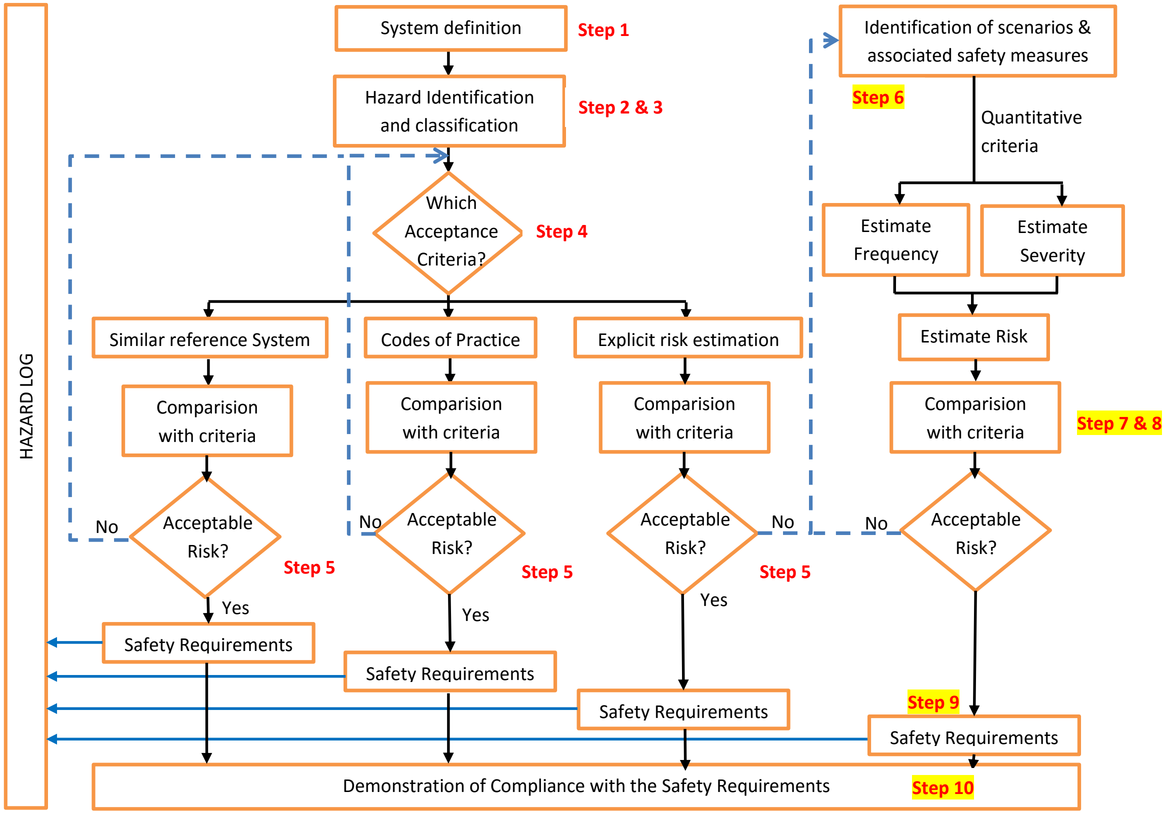
Safety Requirements - Overview

Safety requirements is a global concept for describing all type of measures to be put in place for reducing the severity and/or frequency of risks until getting an acceptable level.

Subsystems contributing somehow to reach an acceptable safety level are managed by Safety Requirements:

- **Functional Safety Requirements** define a function (sensor, treatment and actuator) that contributes to reduce the risk in a given context.
- **Technical Safety Requirements** define design constraints (e.g. the locking system on sliding doors shall withstand a force in the opening direction of 1 200 N)
- **Contextual/Operational Safety Requirements** define a relationship between the system and its environment (e.g. mission profile, staff qualification)

Safety Requirements - Risk Assessment Process

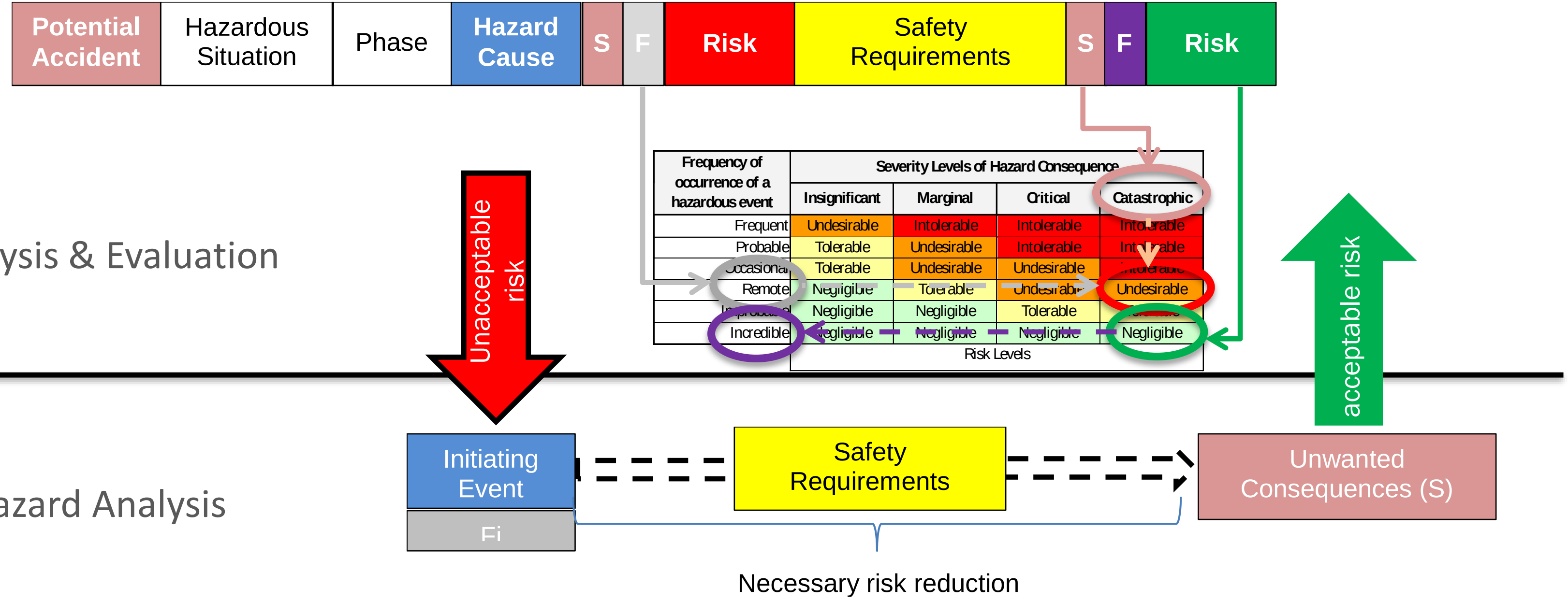


Event Tree Analysis – Link with previous step

The functional safety allocation is anchored to the risk analysis and evaluation

Phase 5
Risk Analysis & Evaluation

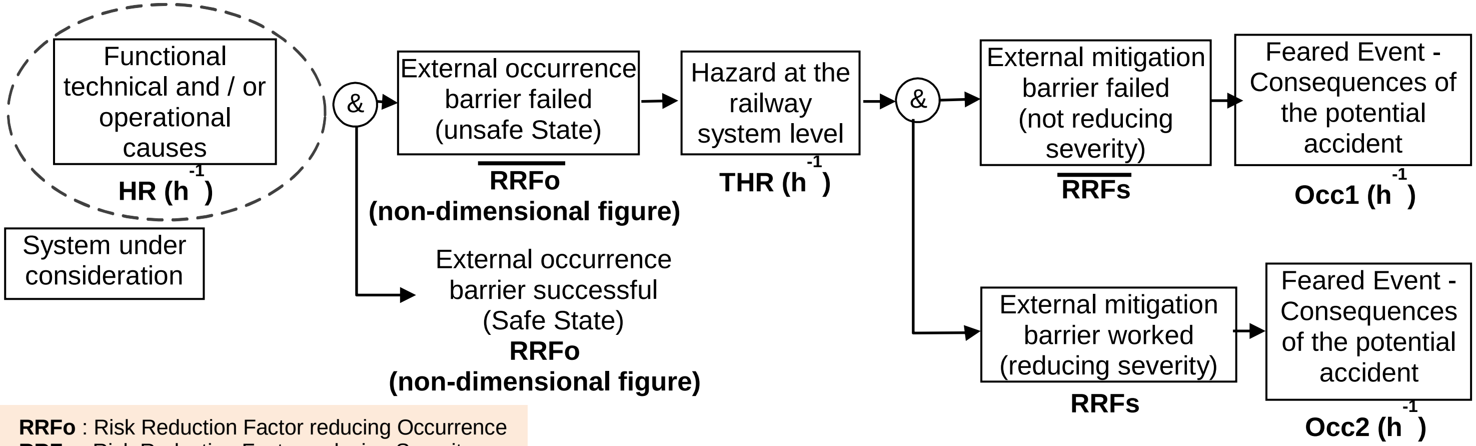
Phase 6
Causal Hazard Analysis



Event Tree Analysis

To model a scenario from an initial event to the accident using an Event Tree Analysis (ETA).

Quantification of the ETA allows to allocate the functional safety requirement (like the SIL):



RRFo : Risk Reduction Factor reducing Occurrence
RRFs : Risk Reduction Factor reducing Severity
Occ1/2 : Frequency of occurrence of the accident

Event Tree Analysis

The efficiency of the barrier in reducing the hazard rate is expressed by the formula:

$$THR = HR \times \prod_{1}^{n} \frac{1}{RRFo_n}$$

With $RRFo_n$ the Risk Reduction Factor of the n **INDEPENDENT BARRIERS** implemented to reduce the occurrence of the hazard/accident coming from a functional technical and / or operational cause.

One can deduce the 2 equations to be resolved :

RRFo : Risk Reduction Factor reducing Occurrence
RRFs : Risk Reduction Factor reducing Severity Oc1/2
: Frequency of occurrence of the accident

$$HR \times \frac{1}{RRFo} \times \frac{1}{RRFs} \leq OCC1$$

$$HR \times \frac{1}{RRFo} \times \left(1 - \frac{1}{RRFs}\right) \leq OCC2$$

From these equations, HR, RRFo and RRFs are defined to reach Occ1 and Occ2 targets.

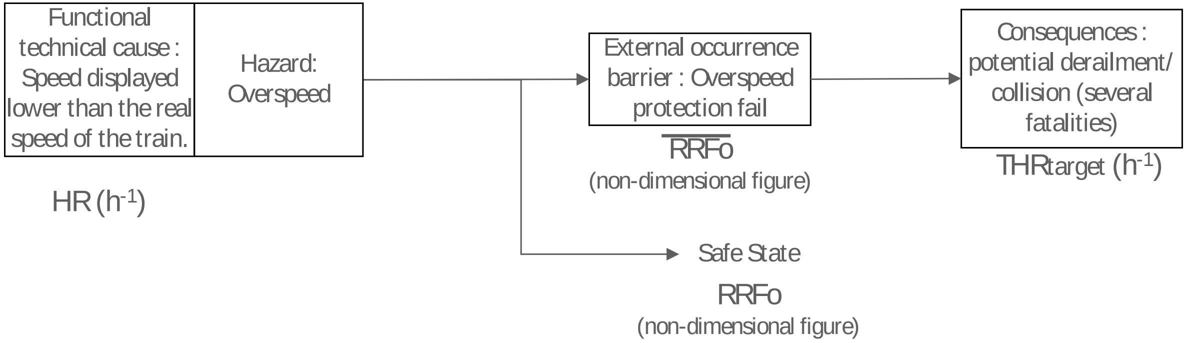
Remark: The HR frequency shall be controlled. If it is not the case (e.g. due to an external cause not controlled), the hazard shall be assumed permanent and the failure of the barrier has to be considered as the actual hazard to be prevented.

RRF versus SIL correspondence

Hazard Rate (HR) [event / hour]	Risk Reduction Factor effectiveness (RRF)	Safety Integrity Level (SIL)
$10^{-9} \leq HR < 10^{-8}$	10 000 < RRF ≤ 100 000	4
10-8 ≤ HR < 10-7	1 000 < RRF ≤ 10 000	3
10-7 ≤ HR < 10-6	100 < RRF ≤ 1 000	2
10-6 ≤ HR < 10-5	10 < RRF ≤ 100	1
10-5 ≤ HR	RRF ≤ 10	Basic Integrity

HR or RRF versus SIL Correspondences

Event Tree Analysis – SIL allocation



Equations to be resolved :

$$THRtarget \geq HR \times \frac{1}{RRFo}$$

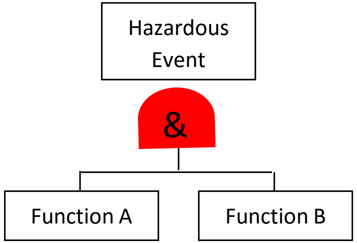
Assuming a THR_{target}≤1E-9/ h, several apportionments are adequate, SIL defined using correspondence table :

HR (h-1)	RRF
5E-7	500
↓ SIL2	↓ SIL2

HR (h-1)	RRF
5e-6	5 000
↓ SIL1	↓ SIL3

SIL allocation W/O RRF

Assuming two independent sub-functions, at allocation Phase (Hazardous Event ≤ HRtarget):



This hazardous event can occurred when Function A and B fail (assuming $HR_X \text{ x } SDT_X \ll 0{,}1$):

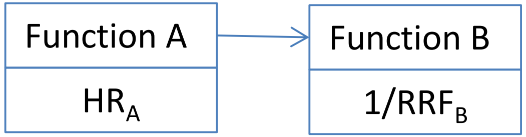
Approach w/o RRF

$$HR_A \times HR_B \times \frac{(SDT_A + SDT_B)}{2} \leq HR_{target}$$

Function A Allocation : HR_A / SIL

Function B Allocation : HR_B / SIL

Approach with RRF



Function A Allocation : HR_A / SIL

Function B Allocation : RRF_B / SIL

INTERNATIONAL RAILWAY SAFETY COUNCIL

SIL allocation with and w/o RRF

Numerical Application with a target < 1E-8/h:

Approach w/o RRF

	Random failure		Systematic Failure
Function A	$TFFR_A$	1E-5/h	Basic Integrity
	$Test_A$	150h	
Function B	$TFFR_B$	1E-5/h	Basic Integrity
	$Test_B$	150h	
Function A	$TFFR_A$	1,4E-6/h	SIL1
	$Test_A$	10000h	
Function B	$TFFR_B$	1,4E-6/h	SIL1
	$Test_B$	10000h	
Function A	$TFFR_A$	3E-7/h	SIL2
	$Test_A$	50000h	
Function B	$TFFR_B$	3E-7/h	SIL2
	$Test_B$	50000h	

Approach with RRF

Systematic Failure	Random failure		
Basic Integrity	$TFFR_A$	1E-5/h	Function A
SIL3	RRF	>1000	Function B
SIL1	$TFFR_A$	1,4E-6/h	Function A
SIL2	RRF	>140	Function B
SIL2	$TFFR_A$	3E-7/h	Function A
SIL1	RRF	>30	Function B

Application

Accident: Fall of passengers on track

Hazardous situation: Door open

Phase: in operation

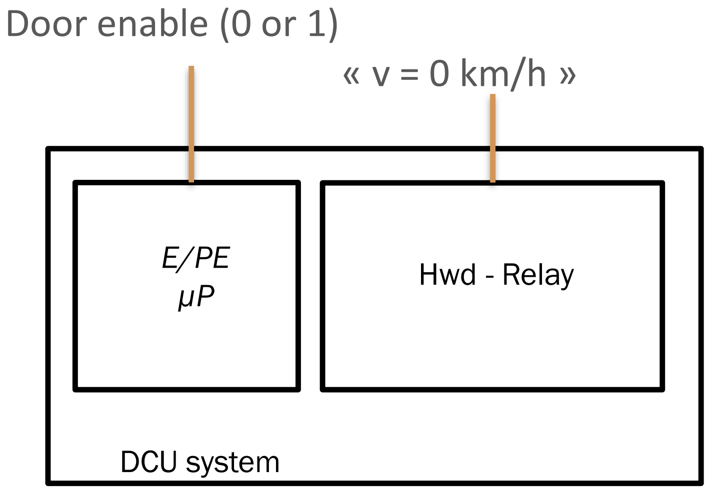
Triggering event: Passengers close to the door

Cause: Door enabled wrongly

Consequence:

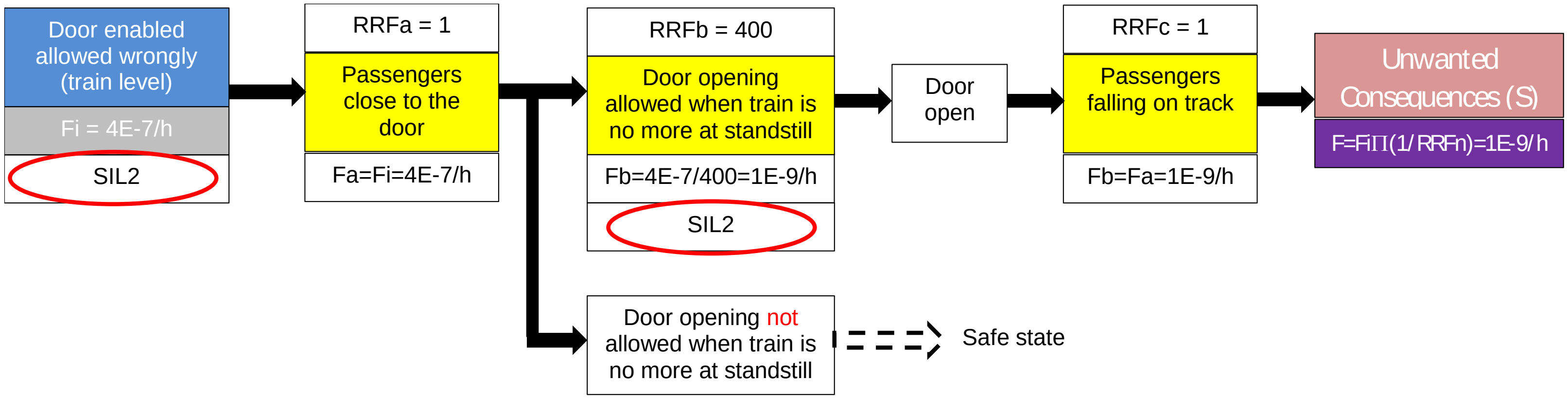
death of several passengers, Target ≤1E-9/h

Single death, Target ≤ 1E-7/h



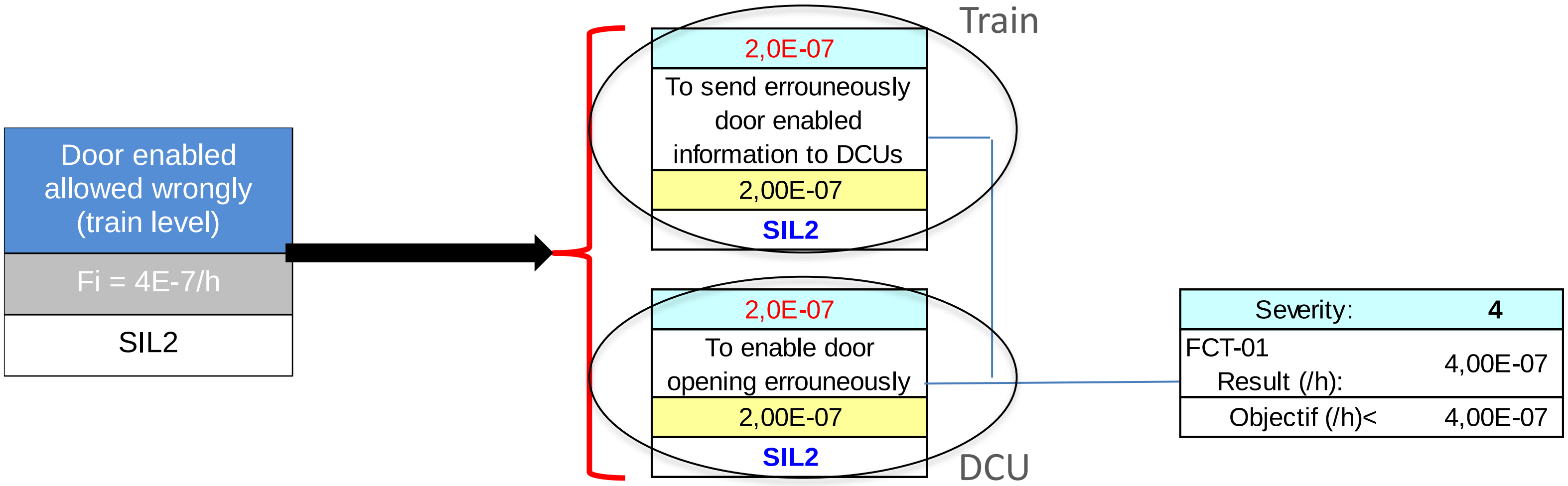
Application

Risk model at train level:



Application

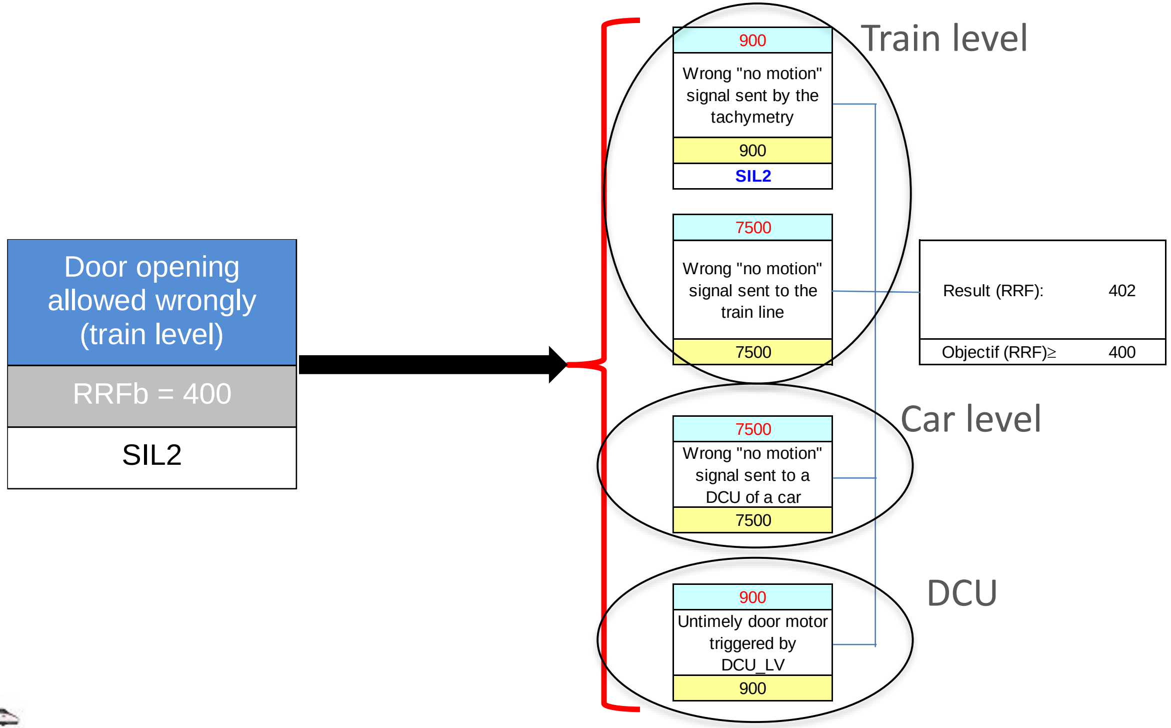
Apportionment of the function “to prevent door enabled without driver action”



INTERNATIONAL RAILWAY SAFETY COUNCIL

Application

Apportionment of the function “to prevent door opening when train is at speed”



Conclusion

The Event Tree and the use of the notion of RRF, allows to:

- Segregate the cause (initial event) from a barrier,
- Model the scenario in a sequential way which is easier to share and challenge by other stakeholders,
- Allocate SIL without specifying the proof test interval,
- Avoid misuse such as allocating a SIL0 based on too short test interval,
- Update event frequency and scenario based on return of experience.