



Annex A

MODURBAN – Annex A for D90

Application of selected MODURBAN safety functions of D86 to MODTRAIN safety analysis method



Investigated Functions:

A.0 Introduction 3

A.1.11 Obstacle Detection in Front of Train 4

A.2.1.1 Door Obstruction Detection 9

A.2.1.2 Gap Supervision/Protection 14

A.2.3 Train Departure Supervision/Management 19

A.4.6 Safe Emergency Brake from OCC 23

A.5.1.2 Emergency Stop Request (from Station Platform) 27

A.5.2 Safe Manual (Emergency) Door Opening 31

A.0 Introduction

The numbering of the investigated function is in reference of the annex of D 86. The numbering of these functions introduced by D86 is kept, to facilitate the traceability of the investigated safety function.

A.1.11 Obstacle Detection in Front of Train

Function Summary Description:

Obstacle Detection in front of train is used in automated operations in order to notice a hit body/object after run over during clearance verification trips to initiate repair/maintenance work.

Operating Modes:

Optional: GOA 1b, 2; Mandatory: GOA 3, 4

MODURBAN-approach:

MODURBAN References:

D77 3.1.7 Supervise Other Safety Related Inputs (external sensors, may include obstacle detection etc.)
D82 3.23.1 Obstacle Detector

Possible Wrong Side Failure:

Undetected run over object/body

Associated Hazards:

If object is hit by train causing damage to first train, obstacle detection cannot prevent damage. If not working, trains on opposite track may also suffer damage.

Possible Consequences/Accidents:

Run over object/body remains in the track area. Trains on opposite track could derail/collide (S3/SL4)

Exposition:

Passengers permanently in trains (A2/E=1)
(In other application first morning trip w/o passengers, A1/E=0,1)

Possible Barriers:

In case of serious damage to detecting train and undetected failure of obstacle detection in front of train, other means signal damaged train (W2/P=0,1)

Possible Consequence Reduction:

Passengers cannot escape consequences, C=1

Table A.1 – Obstacle Detection in front of Train – Method 1

SIL allocation – qualitative	
Defect Obstacle Detection/Train	
S – Damage/Severity	S3
A – Typical Exposition to Hazard	A2
G – Risk Reduction Potential	
W – Probability of Accident	W2
Safety Integrity Level (SIL)	SIL 3

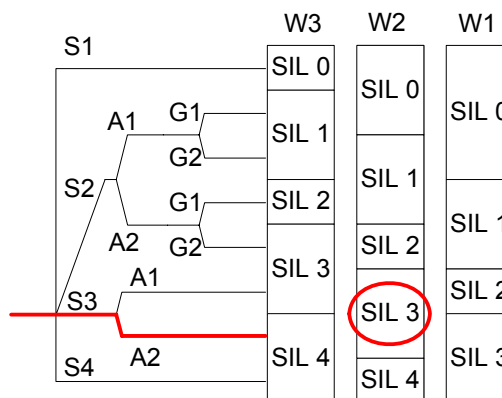


Table A.2 – Obstacle Detection in front of Train – Method 2

SIL allocation – semi quantitative	
Defect Obstacle Detection/Train	
SL – Damage/Severity	SL4
E – Exposition Probability	1
P – Accident Probability	0,1
C – Consequence Reduction	1
THR4/0,1	THR3
Safety Integrity Level (SIL)	-

Tolerable Hazard Rate THR per hour and per function	Safety Integrity Level SIL
THR4: $10^{-9} \leq \text{THR} \leq 10^{-8}$	SIL4
THR3: $10^{-8} \leq \text{THR} \leq 10^{-7}$	SIL3
THR2: $10^{-7} \leq \text{THR} \leq 10^{-6}$	SIL2
THR1: $10^{-6} \leq \text{THR} \leq 10^{-5}$	SIL1

Conclusion:

Obstacle Detection to be realized SIL 3

For preventing trains running into each other, this function should be designed according to SIL 3.

MODTRAIN-approach:

Description: A train runs from A to B. For some reason a body or an object is on this track. The train hits or runs over this object and the obstacle detection means fails to notices the object/body and the train proceeds. The hazard which would emerge is; the undetected object could jeopardise the trains on the opposite track, which could consequently derail or collide with this object. In other words, this obstacle detection means tries to detect every object/body which is hit by a train, in order to prevent the trains on the opposite track to suffer from the damage caused by the object/body. In case, the first train overruns/hits the object undetected, the caused damage could be noticed by the driver. If the object keeps undetected, either the train of the opposite track may be stopped by the driver or the following train might notice the object/body before the train of the opposite track might come too close the undetected object/body.

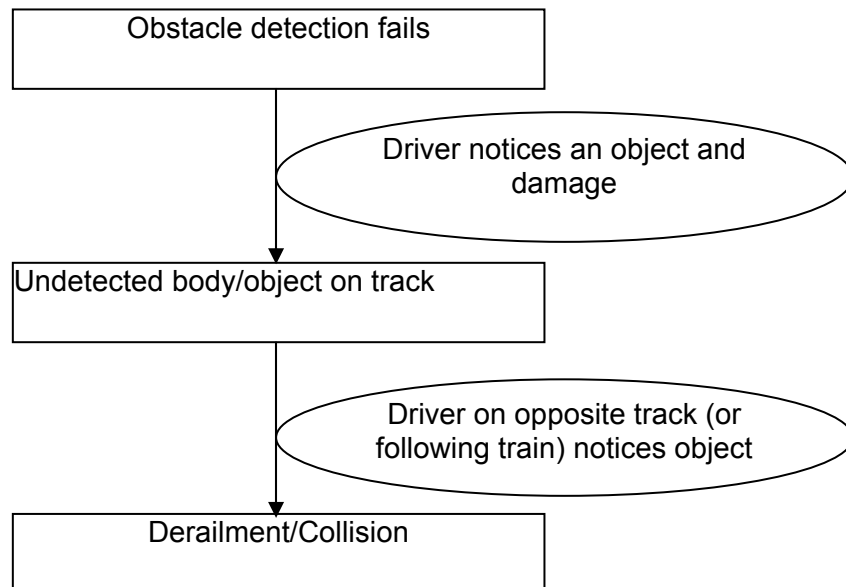


Figure A.1 – Obstacle Detection in Front of Train – MODTRAIN

Accident Context:

- Operational Context = Normal Operation – Train is running [Probability = Frequent]
- Boundary Hazard = [Undetected body/object on track]
- Accident Type = [Derailment, Collision] [Severity = Catastrophic]



Consequence Barriers:

- Consequence Barrier 01 = [Human Factor] [Driver on opposite track notices an object] [Efficiency = Low]
- Consequence Barrier 02 = [Human Factor] [Driver of the following train notices an object] [Efficiency = Low]

Hazard Causes:

- Cause 01 = [Obstacle Detector] (Obstacle detections fails - undetected run over body/object)

Cause Barriers:

- Barrier 01 / Cause 01 = [Human Factor] [Driver notices an object] (damage on train, information to OCC) [Efficiency = High]
- Barrier 02 / Cause 01 = [Mechanical] [Other means detecting run over body/object] [Efficiency = Low]

Final Calculation:

With driver	Without driver
TAR = $10^{-9}/h$	TAR = $10^{-9}/h$
TBHR = $10^{-9}/h / 1 / 1 / 1 = 10^{-9}/h$	TBHR = $10^{-9}/h / 1 = 10^{-9}/h$
THCR = $10^{-9}/h / 0,1 / 1 = 10^{-8}/h$	THCR = $10^{-9}/h / 1 = 10^{-9}/h$
Result: SIL 3	Result: SIL 4

Conclusion:

There are no differences between the two MODURBAN methods.

Without a driver:

The result of the application of MODTRAIN (SIL 4) does not confirm MODURBAN (SIL 3). There is one reason for this difference. The efficiency of cause barrier 02 has been estimated to “low”. This is due to the fact that the efficiency of other mechanical means to detect damages will not exceed the values of an interval of probability of 0% - 60%. So, an efficiency of this barrier could be assumed but, it is too low to change anything. In MODURBAN an efficient barrier has been detected and therefore $P=0,1$. Incidentally, in contrast to the MODTRAIN application, cause barrier 02 acts in MODURBAN as a consequence barrier). Another discussion might arise in the case that the following train approaches the undetected object/body. Several cases are conceivable; the object is not on



the track any more, the train might hit or overrun the object with/without noticing and proceeds or the following train collides or derails due to the object/body.

The assumption that on first morning trips are less passengers was not taken into consideration.

With a driver:

The result is SIL 3. This analysis can be seen as a reference. It is assumed that once an object/body is hit or overran the driver will notice this incident. The driver might see the object and might feel the damage literally. Therefore, cause barrier 01 is estimated with the efficiency category "high".

A.2.1.1 Door Obstruction Detection

Function Summary Description:

During passenger exchange, trains may not depart without authorization (see train departure), passengers need to be protected against being trapped in doors, obstruction needs to be detected.

Operating Modes:

(GOA 2 - 4)

MODURBAN-approach:

MODURBAN References:

D82 3.11.1 Supervise Conditions for Passenger Exchange

Possible Wrong Side Failure:

Obstruction Detection Means signals clearance while doors obstructed, doors lock and keep passenger physically associated.

Associated Hazards:

Train may leave with passenger in door, impacting momentum

Possible Consequences/Accidents:

One fatality S2/SL3

Exposition:

During Crowded Operating Conditions, passengers could be kept in doors during every passenger exchange, A2, E=1

Possible Barriers:

If door interlocking possible with small obstacles present no other barrier can be assumed (W3/P=1)

Possible Consequence Reduction:

Door closing pressure low enough to let passenger in general drag out of closing door (G1, C=0,1)

Table A.3 – Door Obstruction Detection – Method 1

SIL allocation – qualitative	
Passenger Exchange/Door Obstruction	
S – Damage/Severity	S2
A – Typical Exposition to Hazard	A2
G – Risk Reduction Potential	G1
W – Probability of Accident	W3
Safety Integrity Level (SIL)	SIL 2

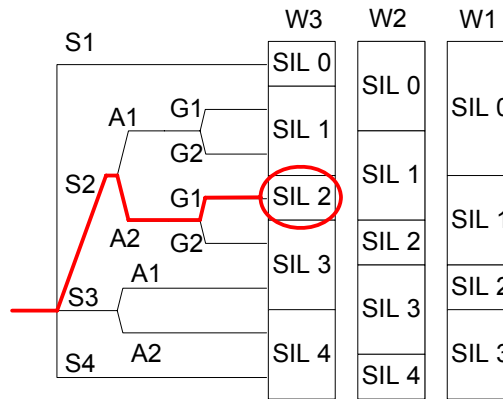


Table A.4 – Door Obstruction Detection – Method 2

SIL allocation – semi quantitative	
Passenger Exchange/Door Obstruction	
SL – Damage/Severity	SL3
E – Exposition Probability	1
P – Accident Probability	1
C – Consequence Reduction	0,1
THR3/0,1	THR2
Safety Integrity Level (SIL)	SIL 2

Tolerable Hazard Rate THR per hour and per function	Safety Integrity Level SIL
THR4: $10^{-9} \leq \text{THR} \leq 10^{-8}$	SIL4
THR3: $10^{-8} \leq \text{THR} \leq 10^{-7}$	SIL3
THR2: $10^{-7} \leq \text{THR} \leq 10^{-6}$	SIL2
THR1: $10^{-6} \leq \text{THR} \leq 10^{-5}$	SIL1

Conclusion:

The Door Obstruction Detection Means shall respect SIL 2

MODTRAIN-approach:

Description: During the passenger exchange the train (or driver) gives the order: “close doors”. To close the doors it is necessary to check if the doors are obstructed. This is done by door obstruction detection. This detection fails and the doors start closing even though passengers are still going in and out. Due to the closing doors a passenger may get trapped in one of the doors. In the worst case, the train starts and drags the trapped passenger. Possible barriers for the miserable situation might be the check of a driver for an ongoing passenger exchange, right before the order to close the doors. Once the passenger is trapped in the doors, the passenger either could free himself or herself due to the limited door closing pressure. Or other passenger or the driver might apply the emergency brake.

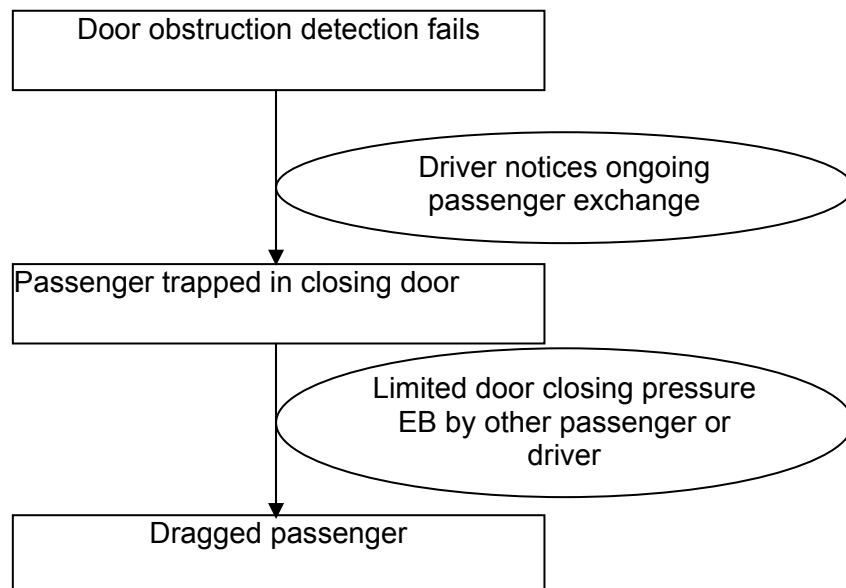


Figure A.2 – Door Obstruction Detection – MODTRAIN

Accident Context:

- Operational Context = Normal Operation – Passenger Transfer/Train Departure – [Probability = Frequent]
- Boundary Hazard = [Passenger trapped in closing door]
- Accident Type = [Dragged passenger] (impacting momentum) [Severity = Critical]

Consequence Barriers:

- Consequence Barrier 01 = [Mechanical] [Door closing force is limited] [Efficiency = Very High]
- Consequence Barrier 02 = [Human Factor] [Other passenger applies emergency brake] [Efficiency = Low]
- Consequence Barrier 03 = [Human Factor] [Driver notices the trapped passenger and applies emergency brake] [Efficiency = Low]

Hazard Causes:

- Cause 01 = [Door obstruction detection] (fails to detect passenger in closing door)

Cause Barriers:

- Barrier 01 / Cause 01 = [Human Factor] [Driver notices ongoing passenger exchange] [Efficiency = Exceptional]

Final Calculation:

With driver	Without driver
TAR = $10^{-9}/h$	TAR = $10^{-9}/h$
TBHR = $10^{-9}/h / 1 / 0,01 / 1 / 1 = 10^{-7}/h$	TBHR = $10^{-9}/h / 1 / 0,01 / 1 = 10^{-7}/h$
THCR = $10^{-7}/h / 0,001 = 10^{-4}/h$	THCR = $10^{-7}/h = 10^{-7}/h$
Result: SIL 0	Result: SIL 2

Conclusion:

There are no differences between the two MODURBAN methods.

Without a driver:

Basically, for the driverless case the MODTRAIN approach (SIL 2) confirms the result of MODURBAN (SIL 2) but, in a different way. Due to adjustments the severity level “critical” is featured with TAR= $10^{-9}/h$, as well as “catastrophic”. For the problem of door obstruction detection MODURBAN uses a value of $10^{-8}/h$, which is the adequate numerical value for “critical”. The second difference is the determination of the efficiency of the first consequence barrier: MODTRAIN asks for the efficiency, this is “very high” because out of 100 trapped passengers for maybe one it might be not possible to free him or herself, whereas, MODURBAN asks for the number of barriers, either one, or two independent barriers. To which extent or quality is not the crucial question, therefore, C=0,1. This is a general



difference. Admittedly, it is arguable whether the efficiency of consequence barrier 01 is “very high” or not. The door closing pressure highly depends on the applied forces.

With a driver:

As a reference the same analysis is made for the case, the train has a driver. Here, the result is SIL 0. During the transition from passenger transfer to train departure the driver is checking the situation all the time, hopefully. Hence, the driver might notice a trapped passenger before the departure of the train. Once the passenger is trapped in the door it will be unlikely that the driver will notice the passenger.

A.2.1.2 Gap Supervision/Protection

Function Summary Description:

During passenger exchange, trains may not depart without authorization (see train departure), passengers need to be protected against falling into gap between train and platform; doors need to detect/prevent obstruction.

Operating Modes:

(GOA 2 - 4)

MODURBAN-approach:

MODURBAN References:

D82 3.11.1 Supervise Conditions for Passenger Exchange

Possible Wrong Side Failure:

Excessive Gap Supervision/Protection Device fails unnoticed

Associated Hazards:

Passenger Trapped in Gap during train departure, passenger gets in contact with third rail

Possible Consequences/Accidents:

One fatality can be the consequence, S2/SL3

Exposition:

Normally, passengers will not fall into gap, A1/E=0,1

Possible Barriers:

Once fallen into gap, passenger could obstruct door or other passenger will use EB (train or platform) – but this can not be conservatively assumed (W3/P=1)

Possible Consequence Reduction:

Passengers may not escape in most cases (no further barrier (G2, C=1)

Table A.5 – Gap Supervision/Protection – Method 1

SIL allocation – qualitative	
Passenger Exchange Gap Bridge (2)	
S – Damage/Severity	S2
A – Typical Exposition to Hazard	A1
G – Risk Reduction Potential	G2
W – Probability of Accident	W3
Safety Integrity Level (SIL)	SIL 1

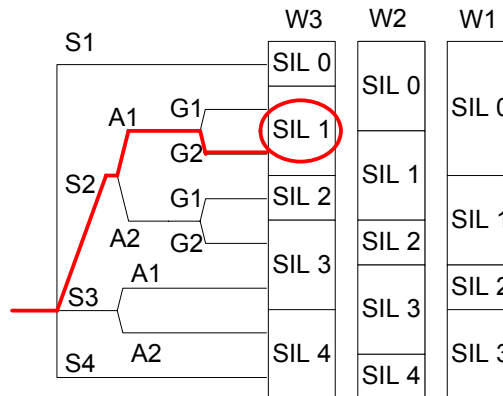


Table A.6 – Gap Supervision/Protection – Method 2

SIL allocation – semi quantitative	
Passenger Exchange Gap Bridge (2)	
SL – Damage/Severity	SL3
E – Exposition Probability	0,1
P – Accident Probability	1
C – Consequence Reduction	1
THR3/0,1	THR2
Safety Integrity Level (SIL)	SIL 2

Tolerable Hazard Rate THR per hour and per function	Safety Integrity Level SIL
THR4: $10^{-9} \leq \text{THR} \leq 10^{-8}$	SIL4
THR3: $10^{-8} \leq \text{THR} \leq 10^{-7}$	SIL3
THR2: $10^{-7} \leq \text{THR} \leq 10^{-6}$	SIL2
THR1: $10^{-6} \leq \text{THR} \leq 10^{-5}$	SIL1

Conclusion:

The Gap Supervision/Protection Means safety level depends to largest extent on the particular situation and needs analysis by every individual operator

MODTRAIN-approach:

Description: The operational context is; a passenger is trapped in the gap between the platform and the train. Even though, this is highly unlikely, it might happen during a passenger exchange. If there is gap supervision and it fails, the following hazard might occur: the train could leave with the passenger still in gap. The possible accident would be an electrocution due to the contact of the third rail or the passenger gets hit by the train. To prevent this accident or hazard several barriers are conceivable: the driver notices the trapped passenger before the train departs, any other passenger applies the emergency brake or the trapped passenger himself or herself could obstruct the doors.

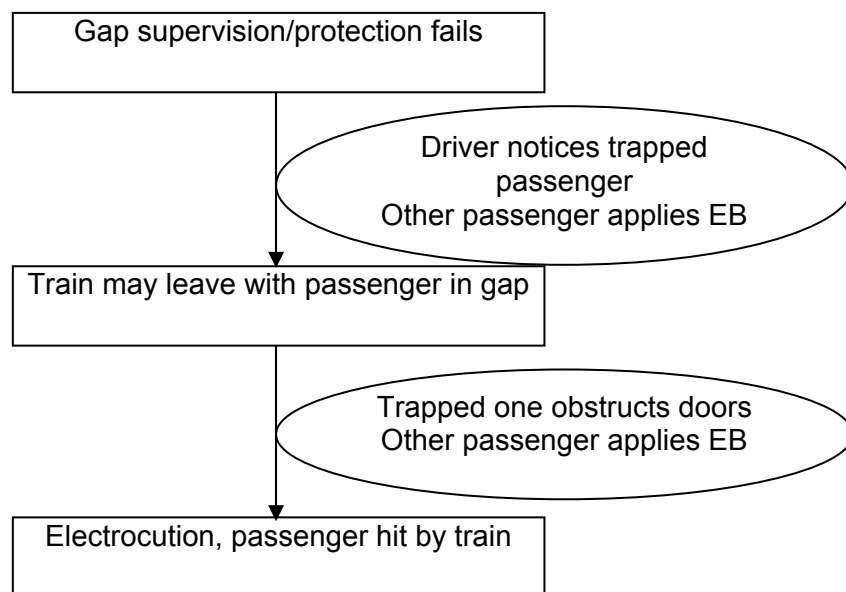


Figure A.3 – Gap Supervision/Protection – MODTRAIN

Accident Context:

- Operational Context = Normal Operation – Train departure/Passenger trapped in gap [Probability = Remote]
- Boundary Hazard = [Train may leave with passenger in gap]
- Accident Type = [Electrocution] (contact with third rail) [Passenger gets hit by departing train] [Severity = Critical]



Consequence Barriers:

- Consequence Barrier 01 = [Human Factor] [Trapped passenger could obstruct door] [Efficiency = Low]
- Consequence Barrier 02 = [Human Factor] [Other passenger could apply emergency brake] [Efficiency = Low]

Hazard Causes:

- Cause 01 = [Gap Supervision/Protection] (fails to notice a trapped passenger)

Cause Barriers:

- Barrier 01 / Cause 01 = [Driver notices the trapped passenger] [Efficiency = High]
- Barrier 02 / Cause 01 = [Human Factor] [Other passenger apply emergency brake] [Efficiency = Low]

Final Calculation:

With driver	Without driver
TAR = $10^{-9}/h$	TAR = $10^{-9}/h$
TBHR = $10^{-9}/h / 0,001 / 1 = 10^{-6}/h$	TBHR = $10^{-9}/h / 0,001 / 1 = 10^{-6}/h$
THCR = $10^{-6}/h / 0,1 / 1 = 10^{-5}/h$	THCR = $10^{-6}/h / 1 = 10^{-6}/h$
Result: SIL 0	Result: SIL 1

Conclusion:

First of all, MODURBAN has two results. Method 1 yields SIL 1, whereas method 2 yields SIL 2. This has methodical reasons.

Without a driver:

MODTRAIN (SIL 1) would confirm the result of method 1 with SIL 1, for the driverless case. Again, the severity level “critical” is featured with the numerical value of $10^{-9}/h$. The operational context is defined in a way that the probability category is “remote”. This has various reasons: the passenger has an instinct of self-preservation and on stations there are several warning signs and announcements regarding the gap. All this prevents the passenger of falling into the gap. In contrast, MODURBAN assumes an exposure of $E=0,1$ only. This value is arguable, because of the reasons, mentioned above, the event a passenger might fall into the gap is definitely very rare. And MODURBAN provides a numerical value for an event with probability of “very rare”. The efficiency of the barriers have no influence to the final calculation, because their efficiency is “low”..



With a driver:

The result is SIL 0. This analysis can be seen as a reference. The probability that a driver will not miss to see a trapped passenger is “high”, which acts as a cause barrier. This means the driver would notice as least 90% of the trapped passengers (cf. table 4: “Efficiency categories for safety barriers [MT]”).



A.2.3 Train Departure Supervision/Management

Function Summary Description:

The CC and Wayside Controls supervise timely and conditioned train departure. Trains depart when all train doors (and platform doors if existing) are unobstructed, closed and locked, and a MAL is constructed.

Operating Modes:

Optional: GOA 1b, 2, 3; Mandatory GOA 4

MODURBAN-approach:

MODURBAN References:

- D77 3.5.2 Supervise Conditions for Start of Train Movement (train doors and PSDs closed and locked)
- D82 3.11.2 Supervise Conditions for Train Departure

Possible Wrong Side Failure:

Undetected CC or Wayside Failure commands/executes untimely when train departure criteria are not fulfilled

Associated Hazards:

Passengers may still exchange at train departure, exposed to momentum transfer

Possible Consequences/Accidents:

Several passengers may get hit by closing doors, dragged by closing doors to end of platform area, between train and platform doors (S3/SL4)

Exposition:

Passengers permanently in doorways during exchange (A2/E=1)

Possible Barriers:

No additional barrier can be conservatively assumed to prevent accident (W3/P=1)

Possible Consequence Reduction:

Passengers cannot escape consequences, G2, C=1



Table A.7 – Train Departure/Supervision/Management – Method 1

SIL allocation – qualitative	
Train Departure Management Supervision	
S – Damage/Severity	S3
A – Typical Exposition to Hazard	A2
G – Risk Reduction Potential	
W – Probability of Accident	W3
Safety Integrity Level (SIL)	SIL 4

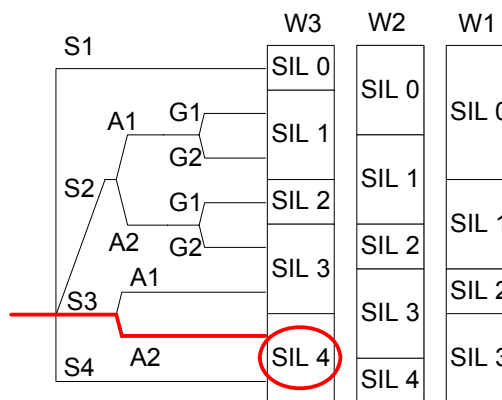


Table A.8 – Train Departure/Supervision/Management – Method 2

SIL allocation – semi quantitative	
Train Departure Management Supervision.	
SL – Damage/Severity	SL4
E – Exposition Probability	1
P – Accident Probability	1
C – Consequence Reduction	1
THR4/1	THR4
Safety Integrity Level (SIL)	SIL 4

Tolerable Hazard Rate THR per hour and per function	Safety Integrity Level SIL
THR4: $10^{-9} \leq \text{THR} \leq 10^{-8}$	SIL4
THR3: $10^{-8} \leq \text{THR} \leq 10^{-7}$	SIL3
THR2: $10^{-7} \leq \text{THR} \leq 10^{-6}$	SIL2
THR1: $10^{-6} \leq \text{THR} \leq 10^{-5}$	SIL1

Conclusion:

The Onboard and Wayside Train Departure Supervision shall assure timely departure under fulfilled criteria with SIL4.

MODTRAIN-approach:

Description: If a train is about to depart, the following criteria have to be fulfilled: all doors have to be unobstructed, closed and locked, and a MAL is constructed. This function is managed by the train departure supervision. If this function fails, in other words, the criteria are actually not fulfilled the hazard of an untimely train departure emerges. Therefore, without any barriers the passengers would get hit and dragged by the train, with catastrophic consequences. But, before the train departs the driver, if existing, might visually check the passenger exchange situation. Once the train is moving other passenger might apply the emergency brake to reduce the severity of the consequences.

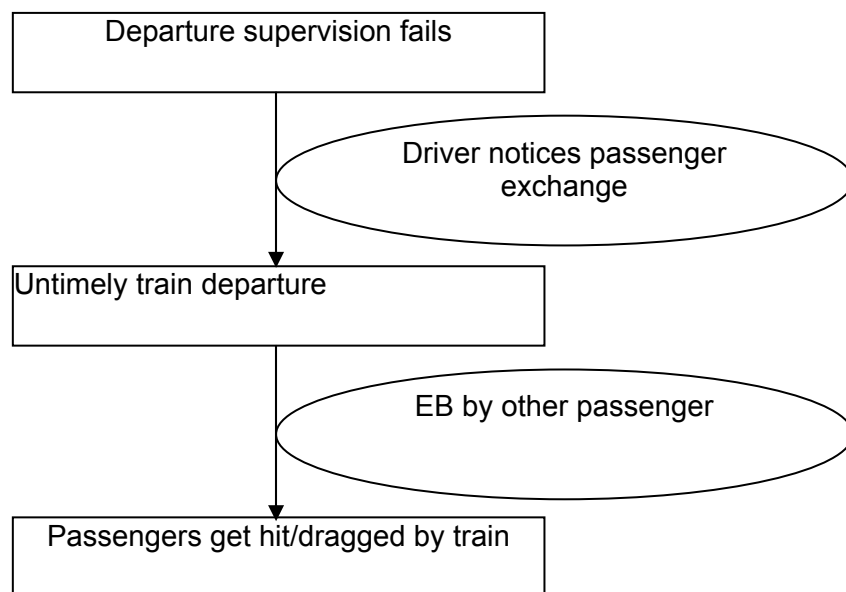


Figure A.4 – Train Departure/Supervision/Management – MODTRAIN

Accident Context:

- Operational Context = Normal Operation – Passenger Transfer [Probability = Frequent]
- Boundary Hazard = [Untimely train departure]
- Accident Type = [Passengers get hit and dragged by the train] [Severity = Catastrophic]

Consequence Barriers:

- Consequence Barrier 01 = [Human Factor] [Other passenger applies emergency brake] [Efficiency = Low]

Hazard Causes:

- Cause 01 = [Train departure supervision/management] (fails, commands untimely train departure)

Cause Barriers:

- Barrier 01 / Cause 01 = [Human Factor] [Driver notices ongoing passenger exchange] [Efficiency = Exceptional]

Final Calculation:

With driver	Without driver
TAR = $10^{-9}/h$	TAR = $10^{-9}/h$
TBHR = $10^{-9}/h / 1 / 1 = 10^{-9}/h$	TBHR = $10^{-9}/h / 1 / 1 = 10^{-9}/h$
THCR = $10^{-9}/h / 0,001 = 10^{-6}/h$	THCR = $10^{-9}/h = 10^{-9}/h$
Result: SIL 1	Result: SIL 4

Conclusion:

There are no differences between the two MODURBAN methods.

Without a driver:

The adjusted MODTRAIN approach (SIL 4) confirms the result of MODURBAN (SIL 4). No efficient barriers can be assumed. Moreover, consequence barrier 01, a passenger would apply the emergency brake if another passenger is hit or dragged by the train, is highly arguable if it is a safety barrier at all.

With a driver:

The result is SIL 1. This case is given as a reference. Cause barrier 01 has been assumed to be “exceptional”, because it should be possible for the driver to unambiguously detect if the passenger exchange is still going on or not.

A.4.6 Safe Emergency Brake from OCC

Function Summary Description:

In MODURBAN, Central Control Staff has a facility to EB one or more trains/sections from OCC in case of emergencies, e.g. Multiple undetected intrusions, evacuations

Operating Modes:

Optional: GOA 1a Mandatory: GOA 1b, 2, 3, 4,

MODURBAN-approach:

MODURBAN References:

D77 3.7.2 Apply Emergency Brakes on Request of Authorised Staff
D82 3.14.3 Emergency Brake Command from the OCC

Possible Wrong Side Failure:

Emergency Equipment fails to EB trains when activated

Associated Hazards:

Trains too close to Safety Target or Obstructions

Possible Consequences/Accidents:

Collisions, derailments S3/SL4

Exposition:

Passengers are permanently in trains but in only rare cases exposed to failures of the central emergency brake activation failures, A1/E=0,1

Possible Barriers:

No additional barrier can be conservatively assumed (W3/P=1)

Possible Consequence Reduction:

Passengers may not be able to escape from full consequences, C=1

Table A.9 – Safe Emergency Brake from OCC – Method 1

SIL allocation – qualitative	
Emergency Brake from OCC	
S – Damage/Severity	S3
A – Typical Exposition to Hazard	A1
G – Risk Reduction Potential	
W – Probability of Accident	W3
Safety Integrity Level (SIL)	SIL 3

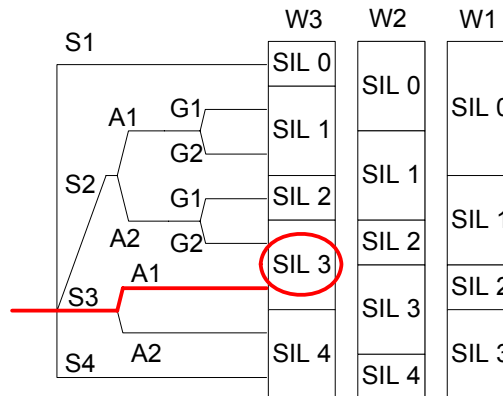


Table A.10 – Safe Emergency Brake from OCC – Method 2

SIL allocation – semi quantitative	
Emergency Brake from OCC	
SL – Damage/Severity	SL4
E – Exposition Probability	0,1
P – Accident Probability	1
C – Consequence Reduction	1
THR4/1	THR4
Safety Integrity Level (SIL)	SIL 4

Tolerable Hazard Rate THR per hour and per function	Safety Integrity Level SIL
THR4: $10^{-9} \leq \text{THR} \leq 10^{-8}$	SIL4
THR3: $10^{-8} \leq \text{THR} \leq 10^{-7}$	SIL3
THR2: $10^{-7} \leq \text{THR} \leq 10^{-6}$	SIL2
THR1: $10^{-6} \leq \text{THR} \leq 10^{-5}$	SIL1

Conclusion:

The Emergency Brake facility for OCC personnel shall be designed according to SIL3, as the use of EB will be a very rare event.

MODTRAIN-approach:

Description: The situation or the operational context is such that the staff of the OCC needs to stop the train on the track via the application of the emergency brake from the OCC. Assumed, the emergency brake would fail to work the train would come too close to certain safety targets. Consequently, this might turn into a collision or derailment. The only barrier which is conceivable is that the driver or passengers on board might notice the situation and apply the emergency brake.

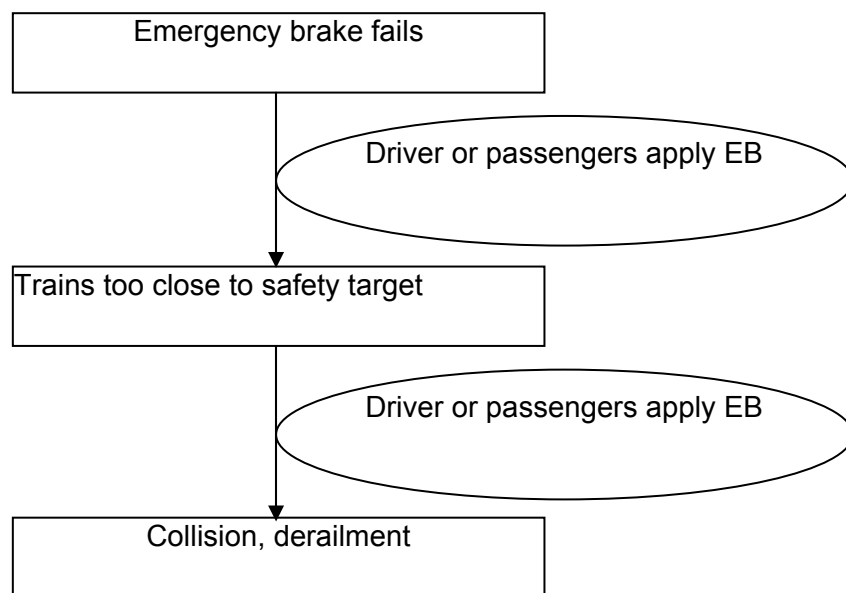


Figure A.5 – Safe Emergency Brake from OCC – MODTRAIN

Accident Context:

- Operational Context = Emergency Situation – Train is running [Probability = Remote]
- Boundary Hazard = [Trains may get too close to safety target or obstructions]
- Accident Type = [Collision, derailment] [Severity = Catastrophic]

Consequence Barriers:

- Consequence Barrier 01 = [Human Factor] [Driver notices critical situation] (applies emergency brake) [Efficiency = Low]
- Consequence Barrier 02 = [Human Factor] [Passenger notices critical situation] (applies emergency brake) [Efficiency = Low]

Hazard Causes:

- Cause 01 = [Emergency brake from OCC] (fails although activated)

Cause Barriers:

- Barrier 01 / Cause 01 = [Human Factor] [Driver notices critical situation] (applies emergency brake) [Efficiency = Low]
- Barrier 02 / Cause 01 = [Human Factor] [Passenger notices critical situation] (applies emergency brake) [Efficiency = Low]

Final Calculation:

With driver	Without driver
TAR = $10^{-9}/h$	TAR = $10^{-9}/h$
TBHR = $10^{-9}/h / 0,001 / 1 / 1 = 10^{-6}/h$	TBHR = $10^{-9}/h / 0,001 / 1 = 10^{-6}/h$
THCR = $10^{-6}/h / 1 / 1 = 10^{-6}/h$	THCR = $10^{-6}/h / 1 = 10^{-6}/h$
Result: SIL 1	Result: SIL 1

Conclusion:

There are no differences between the two MODURBAN methods.

Without a driver:

MODTRAIN (SIL 1) does not confirm the results of MODURBAN (SIL 3). This is mainly due to the assumption that during the application of MODTRAIN, emergency situations occurring only in remote cases. Even though, MODURBAN states “the use of EB will be a very rare event” [MU] and defines the exposure of very rare events with $E=0,01$ it only assumes $E=0,1$. MODTRAIN has the tools to describe the emergency situation as a “remote” event. All safety barriers have been assumed to be “low” regarding the efficiency. This is due to the fact that the critical situation might not be directly recognisable. And a passenger will not interfere at all.

With a driver:

The result is SIL 1. This analysis can be seen as a reference. Both cause barriers are featured with the category “low”, because it might be not recognisable from the train to notice what the problem is. Once a train with a driver approaches a safety target, the driver might apply the emergency brake. In the majority of the cases this will be too late, therefore the efficiency is assumed with “low” as well.

A.5.1.2 Emergency Stop Request (from Station Platform)

Function Summary Description:

Function shall stop approaching trains before entering the Station

Operating Modes:

Mandatory: GOA (1a/b, 2,) 3, 4

MODURBAN References:

D77 3.7.1ff. Supervise Emergency Stop Request

D82 3.14 Emergency Stop Request

Possible Wrong Side Failure:

Failed Emergency Stop although requested

Associated Hazards:

Approaching train in station area too close to passenger on track/over edge

Possible Consequences/Accidents:

Person on track/edge overrun/struck by train S2, SL3

Exposition:

Even at overcrowded stations there are not permanently people within station track or platform edge area, A1/E=0,1

Possible Barriers:

In case of GOA 3/4 additional protection thru GIPS, W2, P=0,1

Possible Consequence Reduction:

Once fallen into track, no escape possible anymore at third rail, low headway (<5min), G2/C=1

Table A.11 – Emergency Stop Request (from Station Platform) – Method 1

SIL allocation – qualitative	
Emergency Stop Request (platform)	
S – Damage/Severity	S2
A – Typical Exposition to Hazard	A1
G – Risk Reduction Potential	G2
W – Probability of Accident	W2
Safety Integrity Level (SIL)	SIL 1

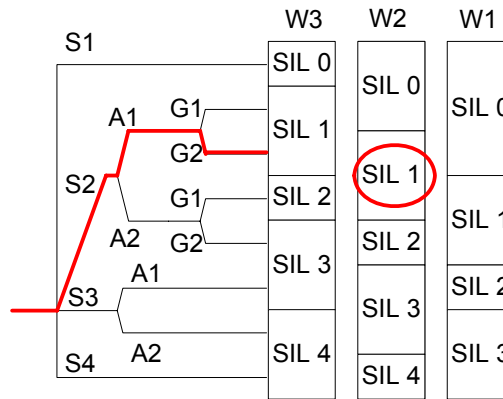


Table A.12 – Emergency Stop Request (from Station Platform) – Method 2

SIL allocation – semi quantitative	
Emergency Stop Request (platform)	
SL – Damage/Severity	SL3
E – Exposition Probability	0,1
P – Accident Probability	0,1
C – Consequence Reduction	1
THR3/0,01	THR1
Safety Integrity Level (SIL)	SIL 1

Tolerable Hazard Rate THR per hour and per function	Safety Integrity Level SIL
THR4: $10^{-9} \leq \text{THR} \leq 10^{-8}$	SIL4
THR3: $10^{-8} \leq \text{THR} \leq 10^{-7}$	SIL3
THR2: $10^{-7} \leq \text{THR} \leq 10^{-6}$	SIL2
THR1: $10^{-6} \leq \text{THR} \leq 10^{-5}$	SIL1

Conclusion:

Emergency Stop Request from station platform in GOA 3/4 shall be designed according to SIL 1.

Nota Bene: Emergency Stop Request is an “on demand Function” – “Emergency Stop Request” is a very rare event – needs to be re-conducted by operator, depends on operation

MODTRAIN-approach:

Description: If one supposes the operational context is that a passenger has been falling into the track, someone on the platform may wish to apply an emergency brake on the station platform to stop a train from entering the station. If this emergency brake fails to react, the consequence of this might be the train overruns or hit this passenger. Two safety barriers can be assumed. On the one hand a guideway intrusion protection/detection system and on the other hand the driver of the berthing train, this might brake the train as soon as possible.

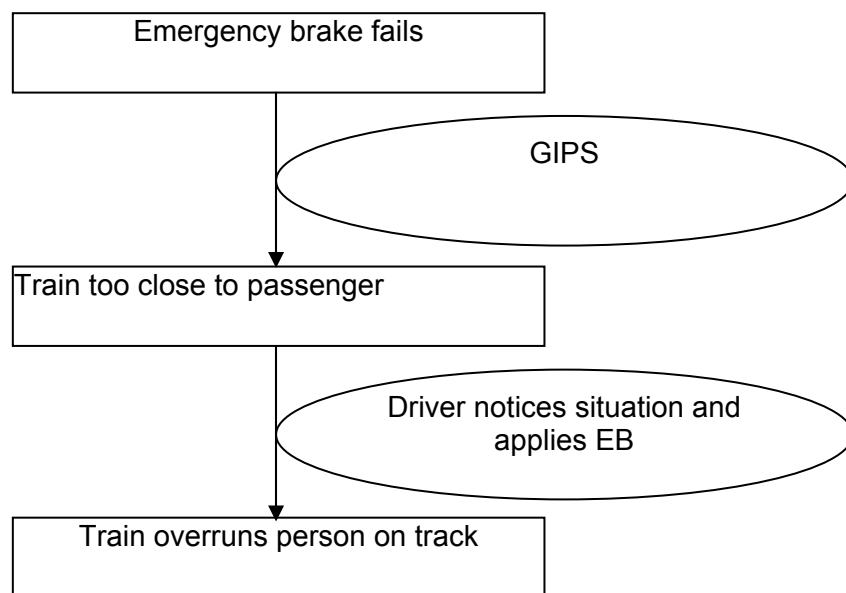


Figure A.6 – Emergency Stop Request (from Station Platform) – MODTRAIN

Accident Context:

- Operational Context = Emergency Situation – Train is berthing/Passenger in trackbed [Probability = Probable]
- Boundary Hazard = [Approaching train too close to passenger]
- Accident Type = [Passenger on track gets overrun by train] [Severity = Critical]

Consequence Barriers:

- Consequence Barrier 01 = [Human Factor] [Driver notices situations and applies emergency brake] [Efficiency = Low]

Hazard Causes:

- Cause 01 = [Emergency stop request] (fails although requested)

Cause Barriers:

- Barrier 01 / Cause 01 = [Mechanical] [Guideway intrusion protection/detection system] [Efficiency = Very High]

Final Calculation:

With driver	Without driver
TAR = $10^{-9}/h$	TAR = $10^{-9}/h$
TBHR = $10^{-9}/h / 0,1 / 1 = 10^{-8}/h$	TBHR = $10^{-9}/h / 0,1 = 10^{-8}/h$
THCR = $10^{-8}/h = 10^{-8}/h$	THCR = $10^{-8}/h / 0,01 = 10^{-6}/h$
Result: SIL 3	Result: SIL 1

Conclusion:

There are no differences between the two MODURBAN methods.

Without a driver:

The application of MODTRAIN (SIL 1) confirms the result of the MODURBAN approach (SIL 1). This had the following reasons. The severity level of “critical” has been assumed with a numerical value of $10^{-9}/h$, which is contrast to MODURBAN where “critical” features the number $10^{-8}/h$. In both approaches the operational context i.e. the exposure to danger has been estimated with 0,1 (“probable”). Different estimations have been made regarding the cause barrier 01. MODURBAN only considers this barrier as one barrier, MODTRAIN asks for the efficiency of the barrier, which has been assumed with a numerical value of 0,01 (“very high”). This is a general difference.

With a driver:

The result is SIL 3. This case has been given as a reference. Instead of the GIPS the drivers efficiency to brake the train appropriately has been assumed with “low”. It will not be possible for the driver to either prevent the accident or reduce the consequences of this accident significantly. Speaking in the intervals of probability of MODTRAIN the drivers efficiency will not exceed approximately 50% (table 4: “Efficiency categories for safety barriers [MT]”).

A.5.2 Safe Manual (Emergency) Door Opening

Function Summary Description:

In case of emergency situations (e.g. Failed Onboard ATP), manual emergency egress shall be authorized after TBD seconds (e.g. 15s) onto the emergency walkway side only and shutdown of third rail

Operating Modes:

GOA 1-4

MODURBAN-approach:

MODURBAN References:

D77 3.5.1 Supervise Door Opening (incl. manual door opening in degraded situation or emergency)

Possible Wrong Side Failure:

Emergency door can be opened before train stop and third rail shutdown or on wrong side

Associated Hazards:

Multiple Passengers exposed to other rail traffic, third rail hazards

Possible Consequences/Accidents:

Collisions, electrocution S3/SL4

Exposition:

Function may have failed between inspections, but passengers are exposed only in the very rare event of emergency, $A1/E=0,01$

Possible Barriers:

No additional barrier can be conservatively assumed ($W3/P=1$)

Possible Consequence Reduction:

No escape or reduction of consequences can be conservatively assumed, $C=1$

Table A.13 – Safe Manual (Emergency) Door Opening – Method 1

SIL allocation – qualitative	
Emergency Door Release	
S – Damage/Severity	S3
A – Typical Exposition to Hazard	A1
G – Risk Reduction Potential	G2
W – Probability of Accident	W3
Safety Integrity Level (SIL)	SIL 3

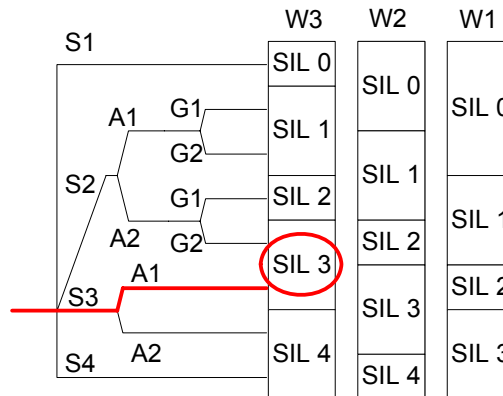


Table A.14 – Safe Manual (Emergency) Door Opening – Method 2

SIL allocation – semi quantitative	
Emergency Door Release	
SL – Damage/Severity	SL4
E – Exposition Probability	0,01
P – Accident Probability	1
C – Consequence Reduction	1
THR4/0,01	THR2
Safety Integrity Level (SIL)	SIL 2

Tolerable Hazard Rate THR per hour and per function	Safety Integrity Level SIL
THR4: $10^{-9} \leq \text{THR} \leq 10^{-8}$	SIL4
THR3: $10^{-8} \leq \text{THR} \leq 10^{-7}$	SIL3
THR2: $10^{-7} \leq \text{THR} \leq 10^{-6}$	SIL2
THR1: $10^{-6} \leq \text{THR} \leq 10^{-5}$	SIL1

Conclusion:

The emergency door release shall be designed according to SIL3/SIL2

Nota Bene:

Emergency Door Release is on-demand function.

MODTRAIN-approach:

Description: In the case of an emergency situation it should be possible to leave the train. If the demanded command to release the doors (for manual emergency opening) is too early and to the wrong side, the passengers might be exposed to other trains or/and the third rail, which is not shut down. This catastrophic case could lead to collision, derailment and electrocution. The only barriers are prudent passengers which are not leaving the train to the wrong side and the driver of other trains noticing the critical situation.

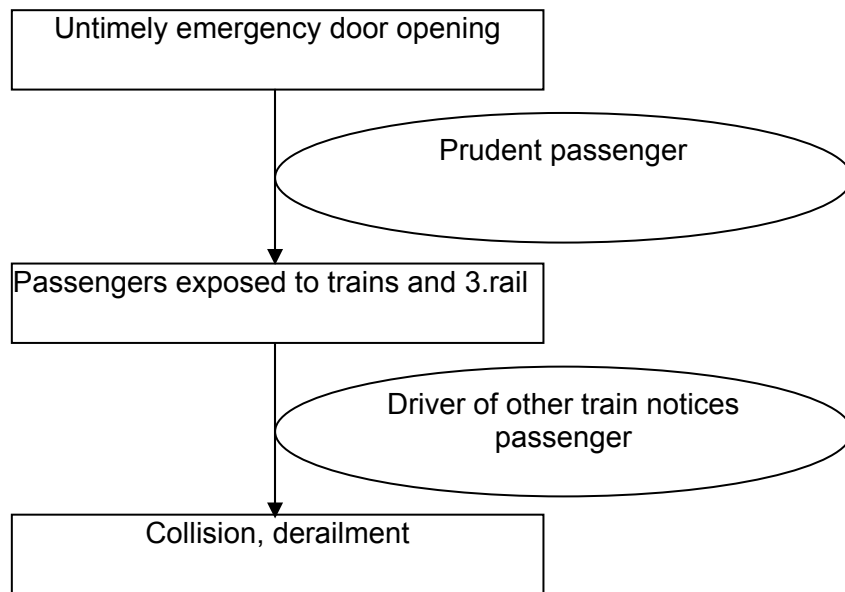


Figure A.7 – Safe Manual (Emergency) Door Opening – MODTRAIN

Accident Context:

- Operational Context = Emergency Situation [Probability = Remote]
- Boundary Hazard = [Passengers exposed to other rail traffic and third rail]
- Accident Type = [Collision, derailment, electrocution] [Severity = Catastrophic]

Consequence Barriers:

- Consequence Barrier 01 = [Human Factor] [Driver of other trains notices passenger on track] [Efficiency = Low]

Hazard Causes:

- Cause 01 = [Safe manual emergency door opening] (emergency doors opens before train stops, third rail not shut down, doors open on wrong side)

Cause Barriers:

- Barrier 01 / Cause 01 = [Human Factor] [Prudent and careful passengers] [Efficiency = Low]

Final Calculation:

With driver	Without driver
TAR = $10^{-9}/h$	TAR = $10^{-9}/h$
TBHR = $10^{-9}/h / 0,001 / 1 = 10^{-6}/h$	TBHR = $10^{-9}/h / 0,001 = 10^{-6}/h$
THCR = $10^{-6}/h / 1 = 10^{-6}/h$	THCR = $10^{-6}/h / 1 = 10^{-6}/h$
Result: SIL 1	Result: SIL 1

Conclusion:

The difference of method 1 and 2 is a general problem.

Without a driver:

Neither of the results of MODURBAN (SIL 2 and SIL 3) is reproduced by the application of the adjusted MODTRAIN (SIL 1) version. The main difference arises from the different category for the operational context and exposure respectively. In this MODTRAIN application an emergency situation like this has been featured with the numerical number of 0,001 which matches with the category “remote”. MODURBAN does not have the fourth category. The most unlikely case can be described with $E=0,01$ only. It is highly unlikely that cause barrier 01 would reduce the THR.

With a driver:

The result is SIL 1. A reference can be seen in this case. Neither of the safety barriers will significantly interfere into the hazard nor the accident.