CHAPTER 8

Risk Analysis of the Charging Procedure of an Electric Road Vehicle

For a practical example of a risk analysis, I choose the charging procedure of an electric road vehicle. I shall take the OPRA analysis and the ensuing hazard identification largely as given, since we have dealt with those aspects in depth already in previous chapters, and concentrate on how the risk may be assessed, given the HazAn. For this analysis, it suffices to have just one OPRA Level. There are of course internal details of the devices which will entail that more levels are needed when the internals of each of the devices are to be considered. It is interesting that the Level 0 objects are all manufactured by different companies, so the Level-0 decomposition is more or less dictated by the social-organisational factors. Further levels would then be company-internal.

This exercise has been abstracted and anonymised from an assessment project conducted by the German electrotechnical standardisation organisation DKE in 2011-2012, led by the author. One of the reasons the DKE undertook such an exercise is the social-organisational factor mentioned above – many different companies need to cooperate to get their devices to work well together to charge an electric vehicle[1].

1 In fact, the organisational situation is far more complicated that this. The current German delegate to the IEC advisory Committee on Safety, Georg Luber, has pointed out that four different IEC Technical Committees have jurisdiction in an electric-vehicle charging process when the charging device is attached to a building and is part of building-electrical circuitry. This is not the case we consider here.

Object (Types)
Interface Electricity Supply/Charging Station
Charging Station/Column
Interface Charging Station/Charging Cable
Charging Cable
Interface Charging Cable/Vehicle
Vehicle

Figure 8.1: Level 0 Physical-Object (Types)

However, the example as presented here should not be taken as the definitive result of an actual HazAn – it is an illustrative example for this book for learning purposes and may well miss some factors important in real electrical life.

I shall consider a practical charging scenario at a public charging station, say an alternating-current conductive charging column on the side of the road, so-called Mode 3 charging [3]. The objects are given in Figure 8.1. Note that a series connection is built between the alternating-current electricity supply on the "grid" and the electric vehicle. It goes from the grid supply to the charging station, from the charging station to the cable, and from the cable to the vehicle. The interfaces between the objects in this series connection are therefore also included. Untypically, in a particular charging station there will be precisely one object of each type being used, so the distinction between objects and their types is moot.

Besides mechanical-physical objects such as those listed, there are various objects involved with the physics and technology of electricity supply – the electrotechnology. These are listed in Figure 8.2.

Object (Types)	
1-phase Alternating Current (AC)	Standard AC, 230-250V in Europe, often limited to 16A
3-phase (Alternating) Current/ Rotary Current	used for systems which require more power, ovens for example. Often 400V
Current	measured in Ampères
Energy Recovery/ Return Current	see Return/Reverse Current
Fault Current	current which flows across a given point of fault resulting from an insulation fault. See also Leakage Current
Frequency	Of AC. In the EU it is 50Hz = 50 cycles per second
Ground (Conductor)	For most electrical devices there is a connection with surrounding objects, sometimes the earth itself. Theoretically, there is a distinction between “ground” and “earth” but this distinction is often ignored by those who are not electrical engineers
Insulation Resistance	The “strength” of insulation.
Leakage Current	electrical current in an unwanted conductive path under normal operating conditions
Mechanical Integrity	mechanically-engineered kit retaining its designed mechanical properties
Mechanical Resistance	resistance of mechanically-engineered kit to mechanical misuse
Neutral Conductor	a specific conductor in 3-phase supply that is intended to act as a neutral voltage to the other 2 conductors
Overcurrent	current greater than that for which the circuit or kit designed in normal operation

Figure 8.2: Level 1 Electrotechnological-Object (Types)

Object (Types)	
Overvoltage	greater electrical tension (voltage) than that for which the circuit or kit is designed in normal operation
Phase	(technical term) argument of the cosine function of a sinusoidal quantity
Residual Current	root mean square value of rotary current flowing over time; alternatively, the algebraic sum of currents in all live conductors at a given time
Return/Reverse Current	sometimes current is intended to flow only one way, e.g., from a charging station to a vehicle. Reverse current flows in the reverse direction from this, contrary to design
Undervoltage	Electrical tension (voltage) lower than designed
Voltage	Electrical tension

Figure 8.3: Level 1 Electrotechnological Objects, continued

8.1 Functional Safety and Nonfunctional Safety

The analyses we are performing in this book concern the functional safety of the systems we analyse. Functional safety concerns the safety of the states and actions concerned directly with the intended functioning of the system. It includes, in this case, the electrical safety of the serial-conducting system from the electrical grid to the vehicle, including the interfaces – likely a plug at the vehicle, although there are some vehicles with integrated cables; maybe a plug on the other end of the cable to fit the charging station if the cable is not included with the charging station; and a permanent connection from charging station to grid. The functional (un)safety of this system does not include, for example, concerns about any sharpness on the edges or at the corners of the charging station, which might injure someone stumbling into it. It does not include the possible effects of toxins present in material used in the construction of any of the devices, or in their paint. The reason is that these features are not part of the defined function of the system, but are part of the construction peripheral to the function.

In this particular example, the analysis does not include any internal reaction of the electric vehicle and its electrics and electronics to the charging procedure, although these are functional components. There are a few reasons for this. First, this part of the analysis could quickly become more complex than what I wish to present here. Second, details of most electric road vehicles' electronics are proprietary. The system from grid to vehicle plug is a collaboration between grid electricity suppliers, charging-station manufacturers, plug manufacturers and cable manufacturers, all of which are different commercial organisations who must cooperate in order to provide an appropriately-safe end-to-end charging system[1].

There are some safety questions which we do not consider in depth here, namely

- the effect of lightning strikes
- general flooding
- earthquakes
- large-area fire
- large-area chemical spill
- vandalism
- protecting a battery of 30-100kWh from unconfined release of energy[2].

Lightning strikes are an electrical-system reality almost everywhere. Unfortunately, so is vandalism, the deliberated intended destruction of parts of a public system providing a public service. The business of confining the energy of the battery of an electric road vehicle under a variety of circumstances is genuinely new and I do not think we can yet say whether this issue has been satisfactorily solved, certainly not on the basis of publicly available information. One could reasonably consider this issue the elephant in the room. I shall ignore it here – this chapter gives an example of a risk analysis, and I make no claim of completeness. These issues are also all

1 These manufacturers chose to look at the issue under the auspices of the DKE in 2011-12.

2 At time of writing, this is the current capacity range of batteries of electric cars on the market. The issues are not trivial. I do have some first-hand experience of working with them. Energy release through fire is at least as big an issue as electrical energy release – lithium-ion batteries are susceptible to so-called "thermal runaway", since the onset for thermal reactions in many electrolytes is less than 200deg C, and temperatures such as this can be reached, for example, at sharp points of electrical discharge within the battery, such as the points of crystals which may build up. The matter is complex. See [7].

present when a charging station is not being used. We are concerned here with the extra-vehicular parts of a charging system in use.

What about vandalism while the charging station is being used? The E/E/PE functional safety standard IEC 61508 says that concern must also be given in the HazAn to "reasonably foreseeable misuse" [2, Subclause 7.4.1.1]. It is not clear whether that includes vandalism of a public object. Does IEC 61508 require that the charging station not expose open conductors when it is damaged? The legal requirement of due diligence on the manufacturer will ensure some designed protection against someone ripping a cable out with bare hands and electrocuting themselves. But if someone drives a large truck into and over the charging station, what then? Such cases are resolved legally in English law by the requirement of reducing risk "as low as reasonably practicable" (ALARP) [1]. They are also resolved socially and technically – it is generally known how to ensure the electrical safety of a public electrically-connected device near a roadway, so one anticipates manufacturers' due diligence will take account of it satisfactorily. Indeed, this is the case with a lot of the hazards which our analysis will turn up – they are dealt with more or less satisfactorily in existing electrical standards.

This is only an example analysis, so I have liberty to choose what is in and what is out. I shall interpret "reasonably foreseeable misuse" to include accidental mechanical damage, but not deliberate destructive attempts.

8.2 Functional-Safety Hazards Not Considered

There are many well-understood aspects of functional safety with electrical systems. These fall under the rubric of "electrical safety". Electrical safety is amongst the most successful of the 19th-century efforts to ensure safety of engineered systems, starting in the 1880's with the introduction of public electric-power supply – Thomas Edison opened the first power station in Britain, the Edison Electric Light Station, at 57 Holborn Viaduct in London, in 1882. The German electrotechnical engineering association, VDE, was founded in 1893 and its original norm on electrical safety, VDE 0100, is valid still today, after myriad updates. Some of the well-understood aspects of electrical safety are

- the possibility of a personal electric shock while connecting elements of the charging system together, or disconnecting them

- the mechanical disturbance of a plug or socket (parts of an interface connection) while current is flowing
- the type and extent of electrical insulation used on various components of the charging system

We will not consider the routine parts of electrical safety, such as the above, which are well-understood and well covered by existing standards on electrical safety. We will, however, consider events and states that may happen during a charging procedure that involve electrical-safety concerns – there are many of them, indeed – but which are not covered by the existing standards.

8.3 Applying HAZOP Guide Words

The HAZOP guide words are reproduced in Figure 8.4. We are concerned here primarily with electrical safety, around which the following guide words seem to lack application:

No no current or no voltage poses no hazard

More we interpret this as fault or leakage current, or as over voltage, and these are explicitly recognised hazards in their own right

Other than interpreted as fault or leakage current, or as overvoltage or over current, and these are explicitly recognised hazards in their own right

Before/After fault, leakage or residual current, either explicitly recognised electrical faults or simply usual phenomena

Faster/Slower has no application to electrical current in this example

So we use just the following guide words:

- More
- Less
- Reverse
- Other than
- Early/late
- Part of

The interpretations are

Guide Word	Interpretation
No	No current, no voltage, no hazard!
More	fault current, overvoltage, overcurrent. Hazards mitigated through electrical safety standards
Less	
As well as	
Part of	
Reverse	
Other than	
Early	
Late	
Before	Fault current, leakage current, over current Hazards mitigated through electrical safety standards
After	Same as for Before
Faster	No application
Slower	No application
Where else	

Figure 8.4: HAZOP Guide Words Again

More/Less concerns

- current: overcurrent/undercurrent
- voltage: overvoltage/undervoltageSpannung
- insulation resistance: too high/too low
- mechanical resistance: the necessary mechanical properties of electrical-system parts are normally laid down in standards

Part of
- Phase: when too few phases are available, for example through wire sewerage or through failure

Reverse
- current: here in particular reverse current

Other than
- voltage, as above
- phase: a relation of two unequal phases
- frequency: a relation of two unequal frequencies

- insulation resistance: with the same interpretation as above
- mechanical resistance: as above
- current: here, leakage current or inappropriate residual current

Early/Late concerns

- protection mechanisms: in particular circuit breakers and reaction times
- mechanical resistance: for example, a built-in break point fractures too slowly or too quickly
- any influence of the charging process on later behaviour of the Vehicle, because a part of the Station is based on digital electronics
- any influence of the charging process on later behaviour of the Charging Station, because a part of the Station is based on digital electronics

Following these considerations, the hazard potential of the possible characteristics listed in Figure 8.5 during charging will be explicitly considered and the hazard potential assessed

Phenomenon	Comment
Overcurrent	Undercurrent is not judged hazardous in any way here
Under/overvoltage	
Too little insulation resistance	too much insulation resistance This is not regarded as hazardous, except in the case in which it leads to leakage current, which already occurs in this list
Too much or too little mechanical resistance in the interfaces/interconnections	Standards already concern themselves with standard or increased protection against mechanical disturbances
Reverse current	Reverse current from the vehicle back into the grid (at the time of original writing, 2012, this was considered inappropriate behaviour; now, grid suppliers are considering how it may be enabled)
Leakage current	Presence or absence. The size of the current is not considered
Failed coherence	Consequences of unequal phasing or frequency over an interconnection

Figure 8.5: Possible Hazardous Circumstances to be Evaluated

8.4 Properties

The properties and relations of the objects in Figure 8.1 are now considered

Interface between the Grid and the Charging Station Much of this is covered by existing electrical-safety standards for permanently connecting devices to the general electricity supply.

- The standards cover *overcurrent* protection well. The grid is physically able to supply current far in excess of what the charging station would require in normal operation, and, given, say, destruction of the charging station when a large truck collides with it, the there is a clear possibility of leakage current from exposed conductors, and this must be shut down. This is a standard type of situation with public electrically-operated devices on

public roads. Nevertheless, the work must be performed as usual.

- The possibility that residual current is present on the neutral conductor following *failed coherence* – resonance or phase-coherence problems – must be investigated and mitigated.

Charging Station The charging station has *insulation resistance* . It must have protection systems for *leakage current* and *overcurrent*. There is a question of what overcurrent may be.

- One interpretation is that it is a current higher than the rated current on the lowest-rated element on the series path Charging Station-(Plug-)Cable-Plug-Vehicle.
- Another interpretation is that the current is higher than the specified charging current. For it is theoretically possible for the charging station to specify and supply a charging current which turns out to be higher than the rated current on, say, a non-standard cable. Cable plugs and sockets are standardised in Europe (a specific 7-pole design from a German design consortium, I understand) and one imagines it is possible for a home hobbyist to obtain two plugs and attach them to whatever cable heshe has, which might be rated lower than industry standards from charging-cable manufacturers.

The second situation is generally regulated socially, through standards, supply and law. And it seems to work quite well. We can thereby assume mitigation of this situation occurs through these mechanisms, as it does in other cases. There will, of course, be exceptions. When considering overcurrent in the Charging Station, I shall consider only the first situation. The consequences of an overcurrent situation backwards on the Grid will not be considered. There are some; they are routinely handled by Grid mechanisms.

The station operates a so-called Control Pilot function as well. A Control Pilot is a separate communications wire in the charging cable to the Vehicle. The Vehicle must also provide appropriate functionality for the Control Pilot, which is described in [3]. We shall not concern ourselves further here with Control Pilot functionality or its HazAn.

Charging Station-Cable Interconnector The Station-Cable connection is equipped with a locking mechanism which

- protects against mechanical disturbance (say, when something falls against it), and
- prevents the plug from being disconnected from the socket during active charging.

It is likely worthwhile to consider a predetermined break point ("rated break point") for the interconnector, so that mechanical disturbance larger than a predetermined limit will break the connector at the rated break point, and enable a predetermined electricity-supply disconnection sequence as it does so, shutting off supply current in an orderly and safe manner. This would help not only in the case in which something or someone falls against the connector, but in the case in which a vehicle drives off without disconnecting, without having released the locking mechanism. Other measures to prevent this might be preferable.

- having a vehicle drive off down the road trailing a cable behind it is some sort of hazardous situation
- however, leaving a forceably-detached Cable attached to the Charging Station with who-knows-what mechanical damage to Cable and Station-Cable Connector is in itself a hazardous situation – what if some new client drives up and attaches to the Cable? A satisfactory internal protection mechanism might recognise a disorderly disconnect, say through a Control Pilot function, and have the Charging Station render itself non-functional pending an inspection. This particular situation, driving off while still connected, has been discussed within standards bodies and the applicable standards (attempt to) regulate it. However, it could be that a vehicle being charged is rammed by a sufficiently large vehicle, an articulated truck, for example. At the time of our consideration of this possibility (2011), this situation had not yet been explicitly accommodated in standards.The "word" from engineers expert in this area is that the situation concerning mechanical integrity is not yet satisfactorily resolved, because there are many contradictory considerations that must be reconciled. A degree of protection against theft is another one I have not considered.

A degree of protection against other environmental influences, such as rain, lightning strike, and chemicals is also necessary.

Charging Cable The Cable has the property of Insulation Resistance, plus specific

electrical resistance properties for each wire in the Cable. The *functional continuity* of the Cable is a very important, maybe essential, property, of which the disruption can have many different causes. For reliability reasons this must be considered very carefully (indeed, this is one reason why there are companies specialising in cable, distinct from the companies specialising in connectors). However, we are performing a risk analysis and consider only the possibility of specifically hazardous situations.

Particular mechanical problems with the Cable can only be identified through visual inspection. This suffices here in order to determine whether the sheath is damaged or retains its integrity. To identify electrical problems (whether with mechanical causes or not) inside the sheath, electrical measurements must be taken.

Cable-Vehicle Connection Under Mode 3 charging, this connection is regarded as identical to the Station-Cable Connection.

Vehicle The Vehicle internally is not part of this inquiry. As far as it manifests itself to the Connector, it has *current*, *voltage*, *current*, *phase*, *frequency*, *electrical resistance* (as measured in Ohms), as well as possibly *leakage current* (the high voltage network of the car is, however, galvanically isolated from the charging system).

8.5 Hazards

From this discussion, and during discussion with domain experts, we came up with the following hazards.

Grid-Station Connector There is a hazard when

1. there is overcurrent or reverse-overcurrent
2. there are combinations of different frequencies (strong harmonics)
3. the characteristics of the current are different (AC and DC)
4. the voltage is different (unforeseen reverse-current into a disconnected grid circuit)
5. the neutral circuit carries current through current characteristics or strong harmonics

Charging Station There is a hazard when

1. there is an insulation failure
2. the characteristics of the current are different (AC and DC)
3. there is an overvoltage through a lightning strike which damages the electronics, in particular the control electronics
4. there is an overcurrent through a lightning strike
5. flammable chemicals are present
6. a voltage is present when, according to the functional stage, it should not be present
7. a charging event has a physical effect on the Charging State which affects its later working

Station-Cable Connector There is a hazard when

1. higher-than-foreseen mechanical force is applied to the Connection
2. lower-than-foreseen structural forces are present (for example, a loose plug-socket fit)
3. there is a mechanical overload of another sort
4. there is higher electrical resistance through dirty or worn contact surfaces

Charging Cable There is a hazard when

1. there is overcurrent (for example, the cable is not able to carry the current which the Vehicle requires and the Charging Station supplies according to Vehicle-Station negotiations.
2. there is too little electrical resistance
3. there is too much electrical resistance
4. there is leakage current (AC or DC)
5. there is an externally-induced hazard (for example, the cable is run over by a heavy object)
6. there is a cable breach or break through high mechanical overloading, for example between Cable and Connector, at an in-cable box (as used in Mode 2 charging, which we are not considering here), in the Cable itself, or at a built-in break point

7. unusual environmental parameters, for example heat sources from an electric motor, or from exhaust or other typical road-vehicle devices such as a catalyser or other parts of an Otto-cycle or Diesel-cycle motor.

Cable-Vehicle Connector There is a hazard when

1. As in Station-Cable Connector
2. As in Station-Cable Connector
3. As in Station-Cable Connector
4. As in Station-Cable Connector
5. Direct current flows, caused by a failure of insulation in a particular area of the electronics of the Charging Station. I am informed that this is a particular issue which arose during standardisation, and which had not been satisfactorily resolved at time of writing (2012). This situation therefore cannot effectively be mitigated here.

Vehicle There is a hazard when

1. the current is different from expected, for example DC current, including leakage current
2. the AC frequency is different from expected
3. there is a different phase sequence by 3-phase reverse current
4. the voltage is different from expected
5. there is overcurrent
6. there is an over voltage
7. there is stray/leakage current
8. there is exceptionally low insulation resistance (with the consequence that leakage current flows to the Vehicle body and chassis)
9. there is unwanted reverse current
10. the frequency is different (leakage current is DC, or often higher-frequency)
11. the charging process has a negative effect on the driving behaviour of the Vehicle after the charging process has ended

8.6 Severity of a Hazard

Charging an electric road vehicle concerns building a circuit from the electricity grid through intermediary devices to the vehicle (and back). The hazards of current flowing in circuits have been relatively well understood for a century or more. The functional severity of those hazards consists in two phenomena:

- electric shock
- fire caused through an electrical fault

That is about it.

In Germany, about 600 people die per year in building fires, and about a third of these are caused by electrical faults [8]. In contrast, an order of magnitude fewer people, about 15 per year, die from electric shock [6]. If we are considering a charging station that is mounted to or inside a building (so-called Mode 1), we may rightly regard the chance of fire as being the main severe consequence, and the chance of electric shock as lesser. If the Vehicle is being charged inside a building, then, say from a high-power charging device permanently mounted to the building, we could consider the consequences of a fire to consist likely in far more damage than an electrocution: more people would be likely killed or injured. This might lead us to the following discrete classification of severity:

- Building fire: Severity 2
- Electric shock: Severity 1
- No damage: Severity 0

However, we are considering a charging station mounted outside, say stand-alone on a street or a parking lot (so-called Mode 3). In this case, any fire is likely to be confined to the (unoccupied) Vehicle, or the Cable, or the Charging Station, and any people in the vicinity are likely to be able to escape rapidly. Damage is thus likely restricted to (minor) property damage. Whereas the possibility of electric shock from the high-power charging system could well injure or kill someone who touches an object through which that current (usual current or leakage) is flowing. Thus in the open-air Charging Station situation we are considering, the severities are

- Electric shock: Severity 2
- Fire: Severity 1

- No damage: Severity 0

Note that in both cases the severities are discrete, and simple.

Hazard analysis attaches their severities to hazards. A risk analysis will often indicate alternative outcomes of hazards, and the severities of those alternative outcomes. I do so in what follows, using a representation of alternative outcomes known as *Event Trees* [4].

The final ingredient in a risk analysis, besides hazards and their severities, is some estimation of the likelihood of a hazard, or a particular consequence of a hazard, occurring. There are almost no statistics on public charging station use for electric vehicles, because there are at the time of writing still not many public charging stations for electric vehicles, and not many purely-electric vehicles on the roads. We consider, then, three discrete likelihoods, in order of frequency/expectation on the basis of your knowledge/your favourite interpretation of likelihood:

- Plausible
- Theoretically Possible
- Implausible

Using these discrete representations of severity and likelihood, we are now able to attach severity, indeed outcomes of varying severity, as well as an estimate of likelihood, to the hazards we have enumerated, using Event Trees. This constitutes a full risk analysis, albeit one that incorporates significant abstraction.

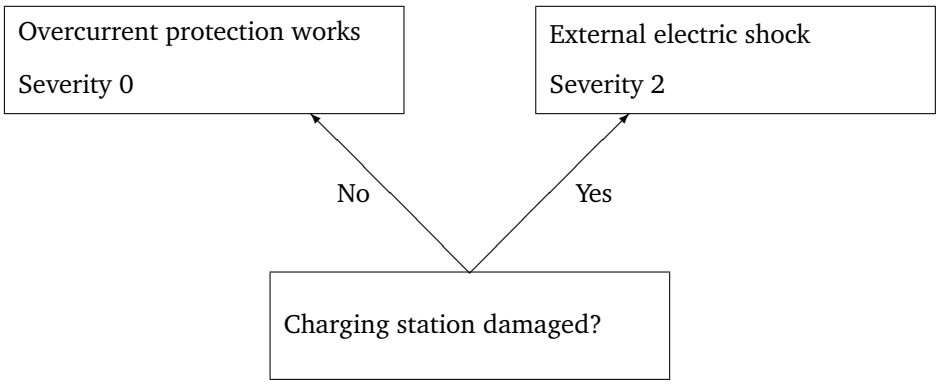
8.7 Risk Analysis via Event Trees

Given that a hazard has occurred, there are behavioural consequences. Things may happen subsequently which elicit the worst possible consequences (usually taken to be the *severity* of the hazard) or less bad consequences. Often there is a decision point, a question “did the following subsequently happen, or not?”, and, depending on the answer yes/no, the outcome is more benign/less benign. Such a elicitation of the consequences and their severity can be shown in the form of a decision tree, called an *event tree*. Event trees are a standard means of representing possible outcomes of hazards [4].

8.7.1 Connection Between Supply & Station

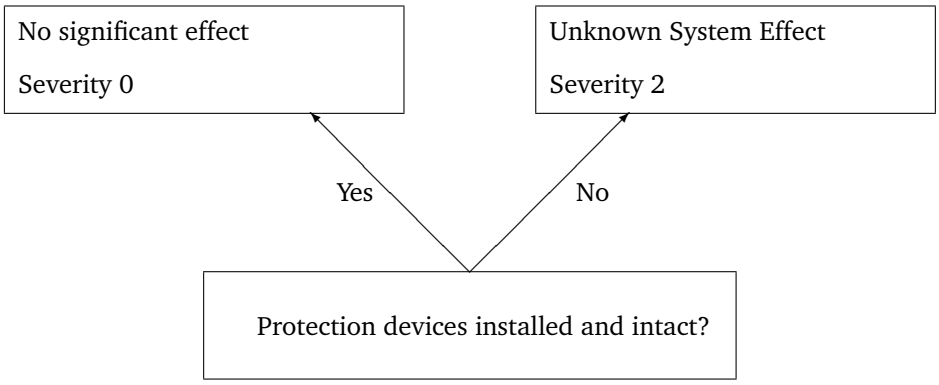
Hazard 1: Overcurrent, reverse-overcurrent

Likelihood: Plausible



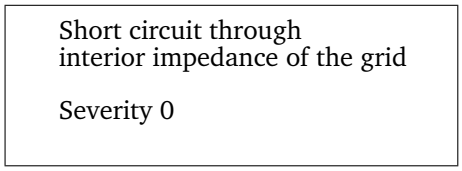
Hazard 2: Combination of different frequencies

Likelihood: Plausible



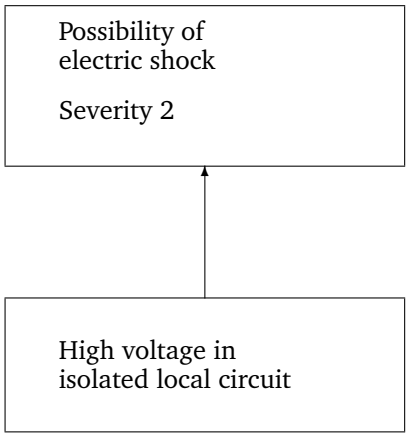
Hazard 3: Current characteristics different

Likelihood: Plausible



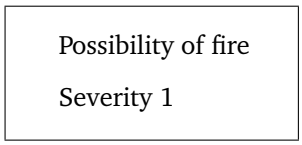
Hazard 4: Reverse-current flow into isolated supply circuit

Likelihood: Theoretically Possible



Hazard 5: Current on Neutral Conductor

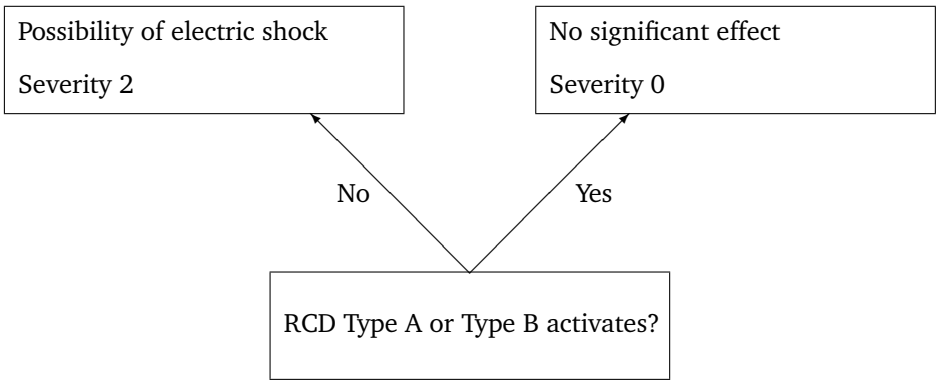
Likelihood: Theoretically Possible



8.7.2 Charging Station

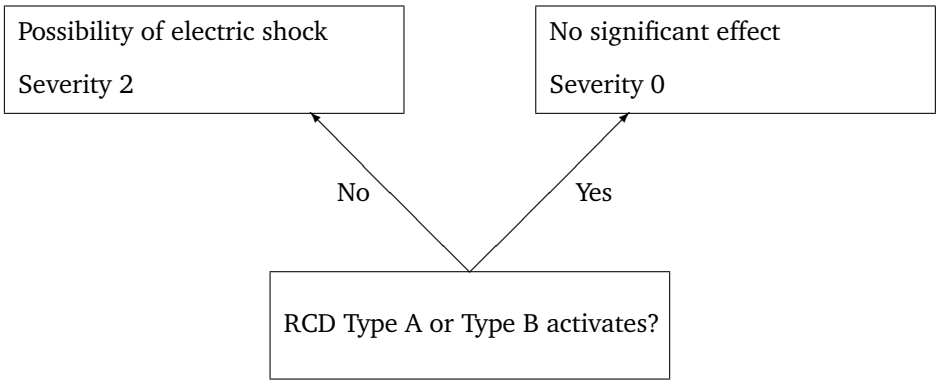
Hazard 1: Insulation failure

Likelihood: Plausible



Hazard 2: Current characteristics different

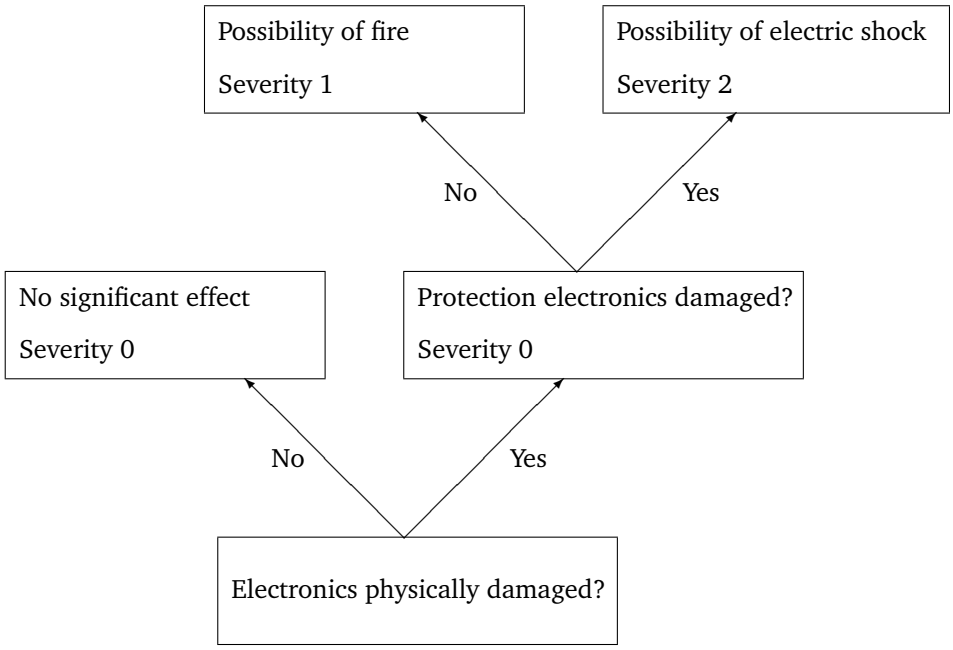
Likelihood: Plausible



Direct current of greater than 6 mA can inhibit the activation of a Type A RCD. Such currents are thus in every case to be avoided. This can be done in the Vehicle, or appropriate protection can be built in to the Charging Station.

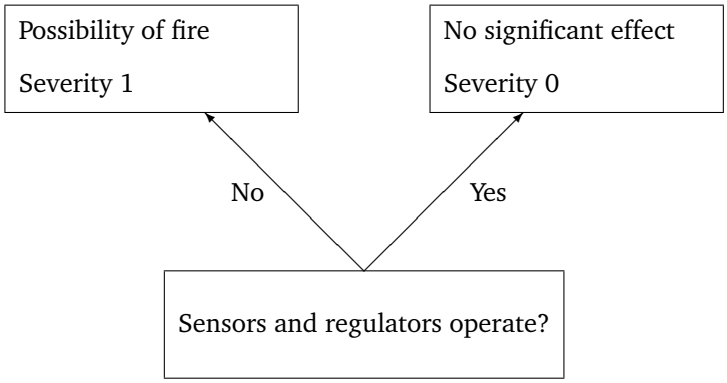
Hazards 3 & 4: Overvoltage (lightning or current) or overcurrent

Likelihood: Plausible



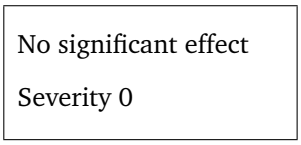
Hazard 5: Inflammable vapours/substance present

Likelihood: Plausible



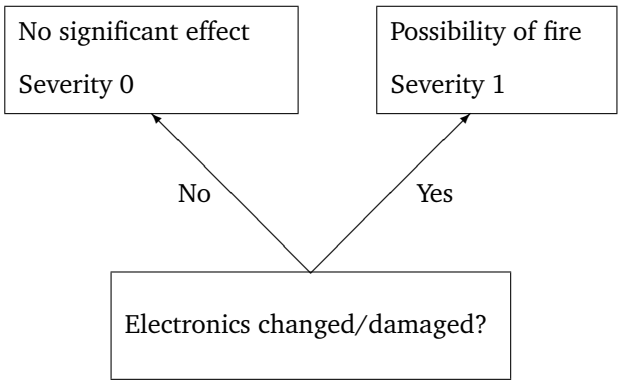
Hazard 6: Unexpected voltage gradient

Likelihood: Plausible



Hazard 7: Charging process affects later operation

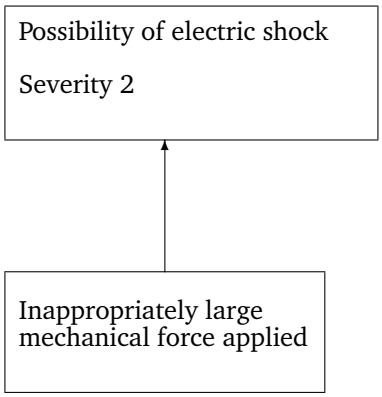
Likelihood: Plausible



8.7.3 Connector Charging Station – Cable

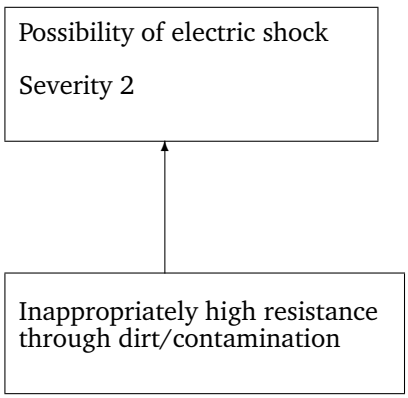
Hazards 1, 2, & 3 can be considered as: inappropriately large mechanical force applied

Likelihood: Plausible



Hazard 4: Inappropriately high resistance through dirt/contamination

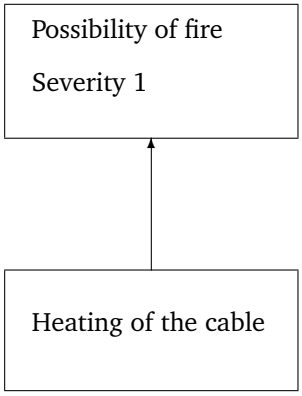
Likelihood: Plausible



8.7.4 Cable

Hazard 1: Too much current for cable capacity

Likelihood: Plausible

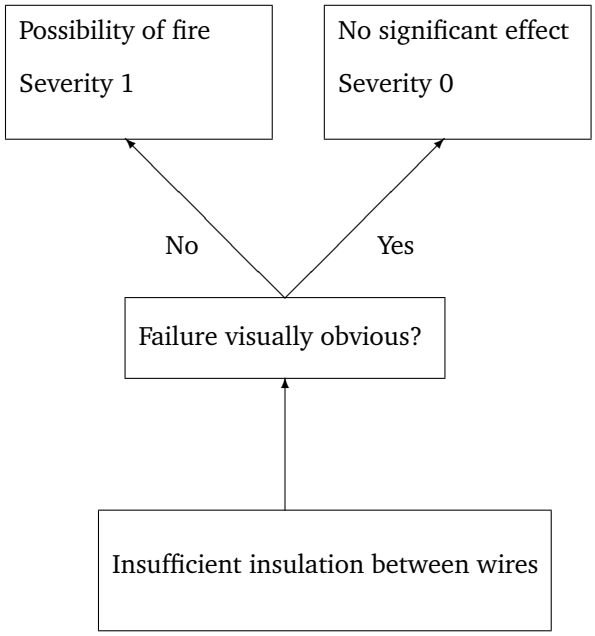


Note 1: such circumstances are usually regulated in applicable electrical standards.

Note 2: overheating of the cable can also lead to overheating of one or both plugs/connectors and consequent damage.

Hazard 2: Insufficient resistance of insulation

Likelihood: Plausible



Note 1: there are two circumstances which can fall under insufficient resistance. First, damage to the outer insulation, which can be ascertained visually and mitigated. Second, damage to inner insulation, which should lead to activation of the Type A RCD protective device.

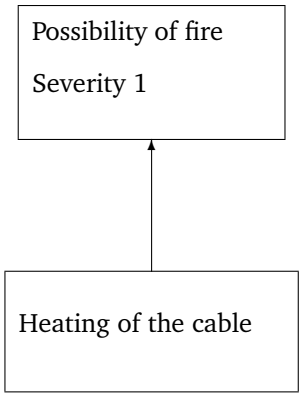
Note 2: Insufficient resistance can also be caused by compression of the cable, or by bending it in too tight a radius. Such circumstances can be caused by, for example, being run over by a vehicle. This occurs with other electrical devices, for example electric lawnmowers come to mind. The situation with road vehicles is different from these in that:

- there is a significantly greater current flow
- the vehicle being charged is significantly heavy
- charging takes place in public areas
- there is the threat of vandalism

- the cable can be rolled over unintentionally during use by a significantly heavy vehicle
- the charging process takes place often, over a relatively long time period
- the charging process is supervised by inexpert users

Hazard 3: Too great throughput resistance

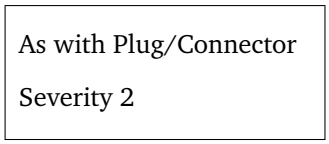
Likelihood: Plausible



Note 1: such situations are usually regulated in applicable electrical standards.

Hazard 4: Different current characteristics

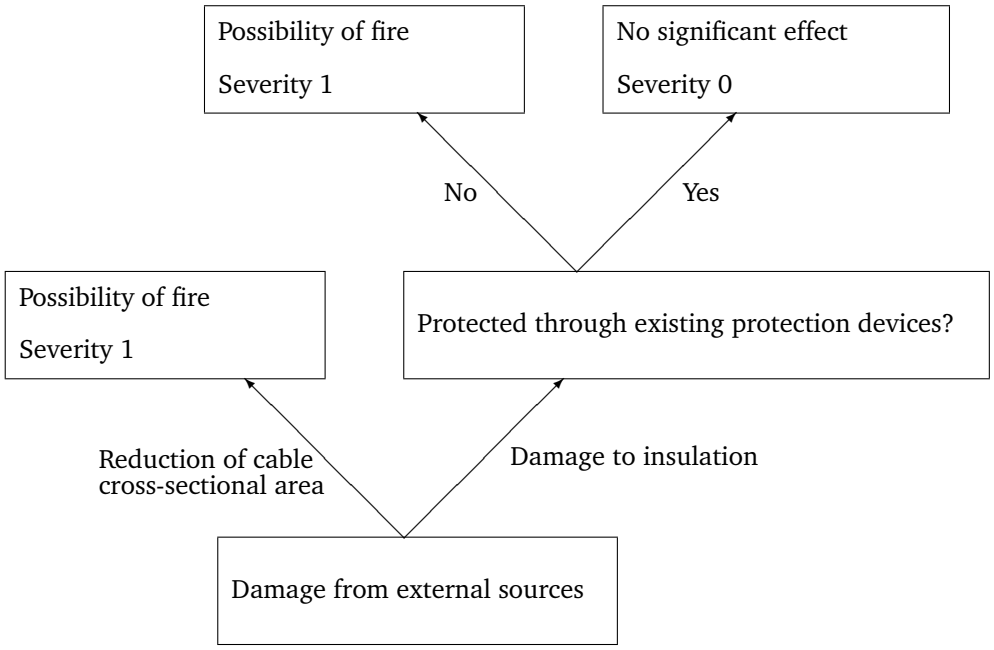
Likelihood: Plausible



Note: The characteristics of heavy current and applicable protections are regulated in applicable standards.

Hazard 5: Damage through external influences

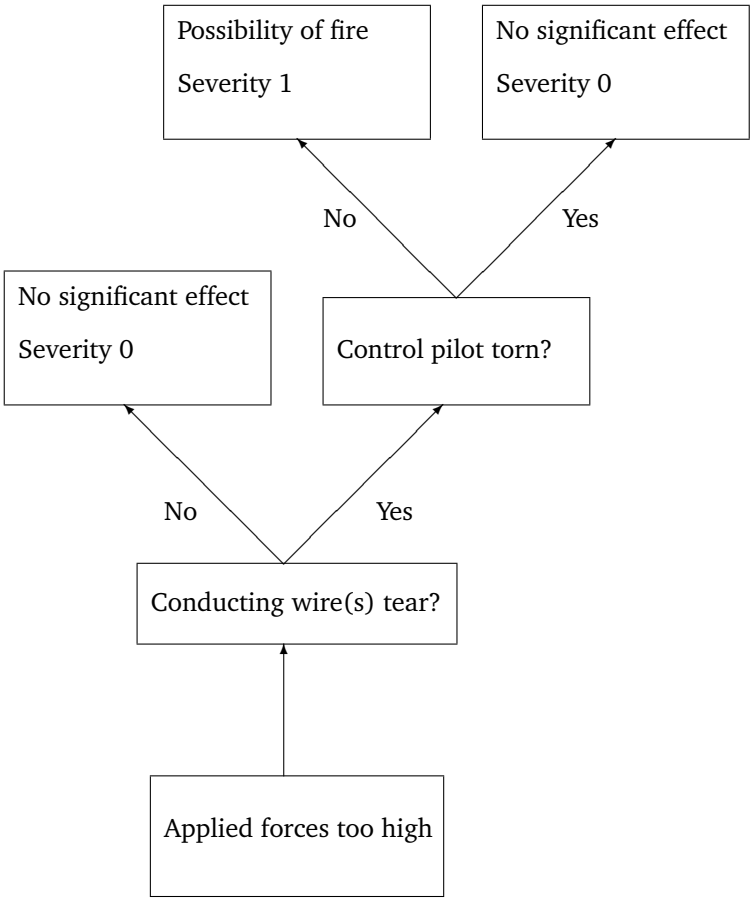
Likelihood: Plausible



Note: The necessary cable robustness is usually regulated in applicable standards.

Hazard 6: Tearing through too high applied forces

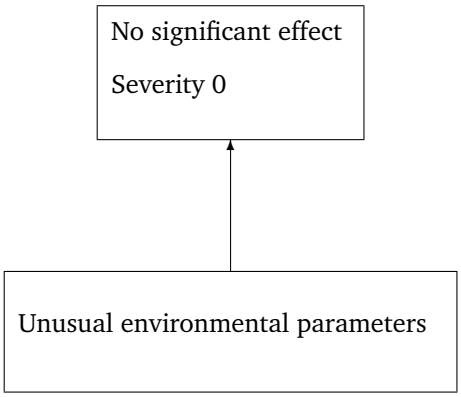
Likelihood: Plausible



Note: The necessary cable robustness is usually regulated in applicable standards.

Hazard 7: Unusual environmental parameters

Likelihood: Plausible



Note: These, such as temperature, wetness, soaking in unusual chemical substances, are usually regulated in applicable standards.

8.7.5 Connector Cable-Vehicle

This is treated the same as Connector Station-Cable, with the following exception:

Hazard: the presence of leakage DC

which can apparently occur at this point through causes which are out of scope here. I understand this is being addressed in standardisation activity.

8.7.6 Vehicle

The Vehicle itself is out of scope for this risk analysis.

8.8 Risk Evaluation

We have enumerated the hazards during charging, and derived simple event trees for severity of outcome, as well as assessed the qualitative likelihood of each class of outcomes of a hazard. The outcomes we have considered are

- No harmful outcome (Severity 0)

Template	EShock	Fire	No Harm
Plausible			
Theoretically possible			
Implausible			

Figure 8.6: Template for a Risk Matrix

- Fire (Severity 1)
- Electric Shock (Severity 2)

and the likelihoods we categorised as

- Implausible
- Theoretically Possible
- Plausible

From these qualitative values, we can build a *risk matrix* template for their combinations as in Figure 8.6. To perform a *risk evaluation*, as it is called by the IEC [5], we need to say which of these combinations are acceptable, and which unacceptable. There may also be some on the margins of acceptability, so maybe we need three values, *acceptable*, *inacceptable* and *marginal*. The *marginal* cases would then be further discussed and resolved into either acceptable or unacceptable.

The easiest part of this matrix to fill out is probably the last row. If a set of outcomes is implausible, then as far as we can tell those outcomes cannot happen and the risk associated with those outcomes is surely acceptable. Further, if no harm is associated with an outcome, then the risk is also acceptable. This gives us the partial matrix of Figure 8.7.

For Mode 3 charging, we are concerned with a charging station standing alone outside. As with most high-power electric devices standing outside in our societies, the risk associated with a plausible chance of electric shock should surely be reduced as far as possible, leading to the risk matrix of Figure 8.8.

This is about all the entries that are obvious. We have taken the risk matrix template and filled out the “obvious” entries.

Now comes the harder part: what about the question marks in Figure 8.8? A chance

Template	EShock	Fire	No Harm
Plausible			Acc
Theoretically possible			Acc
Implausible	Acc	Acc	Acc

Figure 8.7: Risk Matrix With Basic Entries Filled

Template	EShock	Fire	No Harm
Plausible	Inacc	?	Acc
Theoretically possible	?	?	Acc
Implausible	Acc	Acc	Acc

Figure 8.8: Partially-Filled Risk Matrix as a Template for Completion

of electric shock with high-power current could injure someone severely or kill them. All the objects in a charging procedure are standing in the open, and presumably if a fire starts then people can be expected to notice it and move away - they cannot plausibly be inadvertently injured by a fire in the open unless they are proximate to it. But such a fire will cause some damage to property - parts of the charging system and maybe the vehicle itself. One might judge that to be OK - nobody gets hurt, and that is the main thing. On the other hand, suppose you are an exclusive provider of charging facilities for really expensive road vehicles whose owners are exceptionally proud of them. If one is damaged, your business will likely lose all its customers. You might well consider that inacceptable. Is that a matter of safety? Not really. It forms without doubt an inacceptable business risk. But concerning safety, we can well consider it acceptable.

If we consider a plausible fire outcome to a hazard as acceptable, for consistency we must also consider a lesser likelihood of the same outcome acceptable. This leads to the risk matrix in Figure 8.9. There is just one entry left to fill out. We shall leave this to the reader in the exercises.

The situation changes somewhat when we consider Mode 1 charging, in which

Template	EShock	Fire	No Harm
Plausible	Inacc	Acc	Acc
Theoretically possible	?	Acc	Acc
Implausible	Acc	Acc	Acc

Figure 8.9: Almost-Complete Risk Matrix for Mode 3

Template	Fire	EShock	No Harm
Plausible	?	Inacc	Acc
Theoretically possible	?	?	Acc
Implausible	Acc	Acc	Acc

Figure 8.10: Risk Matrix Template for Mode 1

the charging device is affixed to a building. It can happen, and has happened, that the charging system or vehicle exhibits an electrical fault which leads to a fire, and nobody is around to notice the fire taking hold (in the middle of the night, for example). Many more people can be endangered, injured and possibly killed in a building fire, than can plausibly be shocked, as already noted [8]. It seems we need to swap the severities of outcome of fire and electric shock, as in Figure 8.10. But now it becomes easier to fill in at least one of the queries. If a plausible chance of shock is inacceptable, then a similar chance of a worse outcome must also be inacceptable; this entails that a plausible chance of fire is inacceptable. So now we have just two entries left in the risk matrix in Figure 8.11 to fill out for Mode 1 charging. It is left to the reader in the exercises to make a case for acceptability or inacceptability of a theoretically possible chance of fire and a theoretically possible chance of electric shock under Mode 1 charging.

8.8.1 Summary

Notice that there are differences in content between the risk matrix in Figure 8.9 for Mode 3 charging and the risk matrix in Figure 8.11 for Mode 1 charging. The

Template	Fire	EShock	No Harm
Plausible	Inacc	Inacc	Acc
Theoretically possible	?	?	Acc
Implausible	Acc	Acc	Acc

Figure 8.11: Partially-Filled Risk Matrix for Mode 1

plausible risk of fire is acceptable for the first situation and inacceptable for the second. The theoretically possible risk of fire is acceptable for the first situation (because the greater likelihood, "plausible", is acceptable) but is as yet undetermined in the second situation.

Some general principles in constructing risk matrices may be observed, repeated here from Chapter 1:

- If outcome A is acceptable for likelihood L, then it is acceptable for any likelihood category lower than L.
- If outcome A is inacceptable for likelihood L, then it is inacceptable for any likelihood category higher than L.

as well as of course that:

- A risk matrix must be completely filled out
- A filled-out risk matrix should be accompanied by detailed reasoning justifying its entries.

I have not performed the latter two tasks, but the reader will have done so in performing the exercises.

Once it is determined that certain risks are inacceptable, there is a need, a requirement, to avoid or mitigate those risks. The combination of hazards and outcomes which fall into those inacceptable categories need to be revisited, and avoidance and mitigation measures devised, at least until those situations fall into a different, acceptable, category in the matrix. There may also be non-engineering requirements to do something about even those risks which are acceptable, for example according to the ALARP criterion. ALARP stands for "as low as reasonable practicable" and is the legal standard for risk acceptability in English as well as some other law. It can be

regarded as an additional requirement on risk evaluation to that presented by the risk matrix.

8.9 Exercises

1. Is the risk of a theoretically-possible outcome of an electric shock in Mode 3 charging acceptable? Or inacceptable? Make a case for filling out the last entry in the Risk Matrix of Figure **??** either one way or the other. And then make a case for filling it out the other way!
2. Make a case for acceptability or inacceptability of a theoretically possible chance of fire under Mode 1 charging.
3. Make a case for acceptability or inacceptability of a theoretically possible chance of shock under Mode 1 charging. Is it similar to Mode 3, or different?
4. Based on the analysis in this chapter, what are the hazards we most need to protect against? How may we do that?
5. Consider now a Charging Station permanently mounted on a building, say inside a garage. What are the hazards and consequences we most need to protect against? How may we do that?
6. Consider now so-called Mode 2 charging. There is a portable Charging Device, which may be carried in the vehicle, or stored in a building. The Charging Device has one Cable to connect it to a power supply, which may be – usually is – attached to a building, maybe externally or internally. The Charging Device has another Cable to connect it to the Vehicle. Based on the conceptual construction in this chapter, perform a (discrete-)risk analysis of Mode 2 charging. Since the Charging Device is portable, it may be left on the ground where all kinds of things may happen to it. It may be used for charging inside or outside a building, and we have noted two different orderings of severity for “inside” and “outside”.

Bibliography

[1] Health and Safety Executive, *Reducing Risks, Protecting People - R2P2*, UK Health and Safety Executive, various dates. Available from http://www.hse.gov.uk/risk/theory/r2p2.htm , accessed 2017-08-04.

[2] International Electrotechnical Commission, *IEC 61508, Functional safety of electrical/electronic/programmable electronic safety-related systems, Part 1: General requirements*, 2nd Edition, 2010.

[3] International Electrotechnical Commission, *IEC 61851 series (many parts)*, Electric Vehicle Conductive Charging System, many dates.

[4] International Electrotechnical Commission, *IEC 62502, Analysis techniques for dependability - Event tree analysis (ETA)*, 2010.

[5] International Electrotechnical Commission, *ISO/IEC Guide 51 Edition 3, Safety aspects – Guidelines for their inclusion in standards*, Edition 3, 2014.

[6] Georg Luber, *personal communication*, 2012.

[7] Thomas B. Reddy (ed.), *Linden's Handbook of Batteries*, 4th edition, McGraw-Hill, 2011.

[8] Zentralverband Elektrotechnik- und Elektronikindustrie e.V., *Sichere Elektroinfrastruktur - Teil der Energiewende (English: Safe Electrical Infrastructure - Part of Future Energy Supply)*, presentation slides, ZVEI 2012.