Developing a Risk Assessment Process for ANSI B77 Concepts, Challenges, and Objectives

Michael Kingsley, CFSE
Rockwell Automation

Developing a Risk Assessment Process for ANSI B77 - Concepts, Challenges, and Objectives

Michael Kingsley,[1] CFSE

In spring of 2008, at the NSAA National Convention in San Francisco, California, an objective was established by the B77 committee to develop a modern risk assessment process that would be conducive to the needs and culture of the passenger ropeway transportation industry. The objective for this risk assessment process is to provide a structured methodology for manufacturers, engineers, and operators to effectively estimate and evaluate risks associated with passenger ropeway utilization, such that consistent risk mitigation processes and modern functional safety systems could be effectively employed. An Ad Hoc committee was assembled to commence development on this process.

After one year of development activity, respectable progress towards this objective has been made, and a draft version of this process will soon be submitted to the full ANSI B77 committee for draft ballot. This paper will provide a basis for the concepts that have been employed in the process thus far, including the challenges that have surfaced as well as the challenges that lie ahead. In addition, the concept of modern functional safety system design will be discussed in order to support the alignment of this risk assessment process with modern functional safety design standards.

The preliminary risk assessment document, Draft Annex-J, is attached as part of this document to support the topic of the paper.

[1] Job Title: Machine Safety Consultant
Company Name: Rockwell Automation
Address: 728 E. Clearwater Drive
City, Postal Code, Country: Layton, UT 84041 USA
Phone: (801) 648-6524
Fax:
E-mail mlkingsley@ra.rockwell.com

Developing a Risk Assessment Process for ANSI B77 - Concepts, Challenges, and Objectives

Michael Kingsley,[1] CFSE

1. Introduction

Since its inception, the ANSI B77 standard has continued to evolve as a performance-based, prescriptive standard providing a solid foundation for the design and operation of passenger ropeway transportation. Over the past decade, however, the standard has struggled to remain in unison with modern technology development by not appropriately adapting or evolving methods which specify its application in safety-related systems.

A major factor in this struggle has been the lack of a prescribed or referenced method in the standard for assessing risk associated with identified hazards. Without some measure of risk, there is little justification for prescribing relevant or appropriate specifications for risk mitigation measures.

An instance of this limitation is the prescription within the B77 standard[2] for monitoring the acceleration (+/-) component of an operable ropeway. The difficulty with classifying this function lie in the fact that both the hazard severity, and the probability of the hazardous event could vary dramatically depending on various aspects of the ropeway configuration such as size, profile, primary mover type, etc. Theoretical assessment of this hazard results in a range of risk exposures from low to high. Unfortunately, as this function was diligently assessed through many subcommittee meetings, there was no other option then to take the more conservative approach and classify the circuit as a protection circuit[3]. This requires that all installations covered in B77.1 (sections 2, 3, and 4)[2] to have a safety system installed for monitoring this condition that meets the requirements of a Protection Circuit[3]. This results in added costs and complexity that may arguably be considered over-specified for installations that may present negligible to low levels of risk related to this hazard.

This topic also led to the discussion of other prescribed safety functions within the B77 standard that could be debated for similar reasons. As B77 committee members, we often find ourselves with the responsibility of using knowledge, expertise, experience, and ethics in classifying safeguarding measures that we prescribe. We are usually compelled to classify risks in the most conservative direction through purely social considerations alone. In some instances, however,

[1] Job Title:	Machine Safety Consultant
Company Name:	Rockwell Automation
Address:	728 E. Clearwater Drive
City, Postal Code, Country:	Layton, UT 84041 USA
Phone:	(801) 648-6524
Fax:	
E-mail	mlkingsley@ra.rockwell.com

[2] Acceleration/deceleration monitoring. ANSI B77.1-2006, clause(s) 2.2.3.8, 3.2.3.8, 4.2.3.8
[3] Protection Circuit definition and requirements. ANSI B77.1-2006, clause(s) 2.2.3, 3.2.3, 4.2.3

there may be times that identified hazards are dismissed altogether due to the lack of an appropriate classification for low probability risks. Risk assessment and proper functional safety specification will provide the passenger ropeway industry ***a process*** for making consistent, diligent, and ethical determinations to address these types of circumstances.

2. Defining a basis

The first two-day working session for the Risk Assessment AdHoc committee was conducted in August, 2008 in Denver, Colorado. These two days involved getting all team members on the same wavelength, at least with respect to our objectives. This involved team members discussing or presenting on aspects of risk assessment through different viewpoints. A discussion was also shared regarding the overall safety-related system design process. Concepts presented in the Automated People Mover standard[4], and other models were reviewed. There was agreement that although risk assessment is probably the most critical element for establishing the framework for a safety program, it is definitely not the only element for assuring its success. With that said, it is recognized that the potential exists for the incorporation and requirement for a more detailed and complete safety program including additional activities such as planning, management, specification, validation, and maintenance such as that outlined in the APM standard[4]. It was agreed, however, that this exceeded the scope of intent for the Risk Assessment AdHoc committee, at least for now, and that efforts and resources must be focused on the current task of developing only the risk assessment phase at this time.

3. Target objectives for the risk assessment methodology

1) To provide a risk assessment process that will:

    - Document identified hazard exposure to personnel, passengers, and others that may be affected.
    - Provide a technique for estimating risk which is dependent on a straightforward selection of identifiable risk parameters.
    - Based on estimated risk, specify an appropriate measure and its required performance based on a hierarchy of risk reduction measures.
    - In the case where a risk reduction measure is to be implemented as a safety-related control function, a table shall be provided to allow the correlation of required performance or integrity levels established in international mainstream functional safety standards. This will provide the necessary guidance for the design and development of safety related control systems that will take advantage of appropriate state-of-the-art techniques, products, and solutions. This will also eliminate the need for prescriptive functional safety design requirements to be maintained within the B77 standard.

[4] Automated People Mover Standards ANSI/ASCE/T&DI 21-05

2) The process shall incorporate an integration of concepts and methodology implemented across other comparable and relevant industry sector standards. This will help insure that the established framework is justified and substantiated by comparable sectors with respect to risk assessment and functional safety system design.

3) The process shall be formulated around parameters, conditions, and events unique to the passenger ropeway industry.

4) The process shall as best possible achieve some level of congruence with EN passenger ropeway standards with respect to risk assessment and the selection of safeguard performance.

4. Timeline

It was agreed that the overwhelming scope and implication of risk assessment would eventually affect the entire standard. It was unclear, however, how the process would be accepted by the full committee, or the degree of modification that may be required on a continual basis to shape the process into an efficient and usable format. Most importantly, it was agreed that a risk assessment process could potentially have an immediate, positive impact on current standards development activities and that the benefits of this process could feasibly solve many problems that were currently in debate.

With these issues in mind, a decision was made to approach the project in a phased implementation, with the first phase consisting of an Annex[5] that could be voted on and easily implemented as a corrigendum to the base standard. The long term approach would begin targeting areas throughout the standard requiring implicit references as needed where the application of the risk assessment process would be recommended or prescribed. These modifications would be phased into the next major revision of the standard.

This phased approach would allow us in the short term to provide continued maintenance, development, and modification to the annex without causing serious formatting issues with the base standard. The intent will be for the annex to take a normative stance, however, the logistics of when and how the process will take precedence over current prescriptive safeguarding applications has yet to be determined.

5. Research and application

Although many team members brought various expertises, knowledge, and experience that would be critical to development, the foundation of this development is based solidly on mainstream industry standards and state-of-the-art practices. Several risk assessment and functional safety standards were selected for review and adaptation. They are modern, mainstream consensus standards that are accepted and utilized globally in applications of similar relevance and with comparable risk factors. They are all focused on the concept of risk

[5] Proposed Draft Annex J – Safeguarding of passengers and personnel – risk assessment methodology

assessment. These standards, which are listed below, were reviewed and analyzed with respect to concept, structure, philosophy, applicability, and usability:

- ISO 14121-1:2007
  Safety of machinery / Risk Assessment
- ANSI/RIA R15.06:1999 / Clause 9, Risk Assessment
  Safety requirements for industrial robots and robot systems
- ISO 13849-1:2006
  Safety of machinery / Safety related parts of control systems
- IEC 62061:2005 –
  Safety of machinery / Functional safety of safety-related electrical/electronic/programmable electronic control systems.
- ANSI/ASCE/T&DI 21-05
  Automated People Mover Standards – Part 1
- EN 13243:2004 / Annex's A, B, and C
  Safety Requirements for cableway installations designed to carry persons
- ANSI/PMMI B155.1-2006
  Safety requirements for packaging and packaging-related converting machinery

During this research, we have focused on particular aspects of different methodologies and proceeded to apply concepts from these standards that helped meet the overall objectives of the methodology. Processes which provided an abbreviated approach (10 – 20 pages) offered an aspect of user-friendliness that should prove beneficial over the short term. Our approach would shoot for similar length and content. Processes that were too abbreviated (1-2 pages) would prove to be too vague and not provide enough guidance or example that would be necessary for this industry. Also considered was whether or not to simply reference an external risk assessment standard. Through review and discussion, it was obvious that relevant risk assessment methodologies that currently existed were highly focused on general machinery application and some correlation would have to be made with respect to terminology. Experience within the group also identified that this would make the process too complex, or highly unusable for the majority of those required to implement it. So the decision to develop a custom methodology fitting more closely the requirements of the passenger ropeway industry was made. It is possible that informative references could be added to the annex referencing additional risk assessment standards to provide further reference and resources for those looking for further qualitative guidance. This will be considered as development continues.

The primary framework and body of the Annex-J[5] process has been derived from parts of ANSI/RIA R15.06, Safety requirements for robots and robot systems. This standard offers a very straightforward approach to risk assessment that included requirements and responsibilities for both the manufacturer of the equipment as well as the end user. Structure and terminology was modified and various concepts have been expanded in order to provide applicability. The R15.06 process follows a standard iterative risk assessment process and is closely coupled to a widely understood hierarchy of risk mitigation techniques. This allowed us to create a "hierarchy of risk mitigation measures" that would provide guidance on the appropriate application of mitigation techniques other than safety-related controls, such as awareness indicators, signs, procedures, training, personal protective equipment, information for use, and others.

Several standards were assessed that offered different graph and matrix-based processes for estimating risk. Since passenger ropeway related hazards would encompass a wide range of event conditions for both personnel and passenger related interaction, we looked for a process which entailed more than two discrete choices for each individual risk parameter such as severity, frequency of occurrence, avoidance, and so forth. Having more possibilities to select from allows for a more accurate estimation and also eliminates more instances of having to make "fuzzy" decisions due to selections that may fall somewhere between two selections. Also considered was the number and relevance of possible risk categories that could be derived through the estimation and how these risk categories would align with various other functional safety standards as well as the European passenger ropeway standards.

The risk parameter selection and estimation method is highly based on the methodology outlined in IEC 62061:2005/Annex A. Terminology and nomenclature has been modified for applicability and various elements were modified in certain instances in an attempt to simplify parameter selection. The basic structure was maintained such that ultimate determination of risk reduction levels (RRLs) would directly coincide with established SIL (Safety Integrity Level) terminology utilized in the IEC 62061:2005 standard. In turn, SILs can be correlated to PLs (Performance Levels) via ISO 13849-1:2006 / Table 4, and likewise to AK (Requirements Class) via the table in EN 13243:2004 / Annex B. The correlation of RRLs to either SIL or PL has also been provided in Draft Annex-J[5] / Table J.8 for simplicity.

6. Challenges

The main challenges of developing this process have primarily revolved around taking such a broad and complex subject and developing an abstract process that was simple to use and directly applicable to the industry. If it is difficult to apply, or its benefits are not well understood, then it will experience resistance. The process simply needs to be distributed as its real usefulness cannot be understood, assessed, or improved until it has been practiced by the very people that will be required to apply and/or verify it. As with most standards or new concepts, it will not be perfect at inception, and for that matter, may never be perfect. Our challenge moving forward with this will not be known until the first wave of feedback is provided by the committee.

A further challenge that exists, and is experienced with most risk assessment processes in practice, is in the determination of acceptable risk. **At what point in the process, for a particular hazard, have the applied risk mitigation technique(s) lowered the risk to some acceptable level?** This concept is addressed in part when the risk mitigation is to be provided through a safety-related control function (functional safety). In this case, a safety function (safety circuit) is designed which will detect the hazardous conditions and control potential hazardous energy sources effectively eliminating the hazardous event. The safety function, however, shall be designed in accordance with either IEC 62061:2005 or ISO 13849-1:2006 to the selected SIL or PL, which includes suitable requirements for fault tolerance (redundancy), fault diagnostics, common cause failures, and very importantly failure rate probability. Also covered are stringent coding standards and validation of safety rated application software. Meeting the sum of these requirements per the standard verifies that the function will achieve a target PFH_d (probability of dangerous failure per hour) value, and in turn providing a quantitative level of risk reduction. An additional justification to SILs and PLs here is with the APM standard[4], where acceptable risk is ultimately parameterized by quantitative measure in MTBHE (mean time between hazardous events). In comparison, a catastrophic or critical hazard may be deemed acceptable per the APM standard[4] (with notification to the AHJ) if the applied safety system can assure a MTBHE of at least 100 million hours (1 x 10^8 hours). This is the highest MTBHE specified and classifies the possibility of the hazardous event occurring as "improbable". Conversely, SIL 3 and PLe safety functions are in the order of 1 X 10^8 hours between dangerous failures (hazardous events).

For the cases in which complementary measures other than safety-related control functions have been applied, such as fixed guarding, signs, warning indicators, procedures, etc., or the functional safety system will not completely control the hazard, then one must evaluate any residual risk. This is accomplished by re-applying the risk estimation process, modifying any risk parameters that were effectively reduced, and re-calculating residual risk. In this case, there is no fine line drawn in the sand. Logic might establish that an RRL=Low would be the target, but only under circumstances in which at least one iterative step of reduction has been applied.

In comparison to some of the other standards reviewed, the ANSI R15.06 standard requires, after estimation, at least one application of risk mitigation for any hazard identified, regardless of risk category. However, once one pass has been made, if the risk level falls into categories with minor severity (first aid or less) harm, then acceptable risk is assumed.

Furthermore, in the packaging standard, ANSI B155.1-2006, a definition is provided for acceptable risk and is given (in part) as the following: *The expression "acceptable risk" refers to the level at which further risk reduction will not result in significant reduction in risk; or additional expenditure will not result in significant advantages of increased safety.* Also mentioned as a note in this definition is; *the user and supplier may have different levels of acceptable risk*. Although this entire definition could be highly construed and leaves a high degree of gray area, it at least provides a basis for ones thinking as they work through the process.

Tolerable (acceptable) risk is a topic covering a very large scope of probabilistic thinking, a wide range of theory and philosophy, and involves a highly complex mathematical basis. The beauty of applying IEC 62061:2005 or ISO 13849-1:2006 is that tolerable risk is not only taken care of inherently through SILs and PLs, it has been almost completely hidden to provide usability.

7. Moving forward

An objective that will hopefully be met and incorporated prior to a final vote on the draft would be an additional table or section providing numerous worked examples of applying this process. This has been similarly provided in EN 13243:2004 / Annex C, and seems to serve as a very valuable guide.

Long term research and review will begin regarding the incorporation of advanced topics on tolerable risk, such as ALARP (as low as reasonably possible) as well as further risk reduction measures to include advanced topics in LOPA (layer of protection analysis) as they are deemed applicable. These are topics that be reference in IEC 61508-5:1998, IEC 61511-3:2004, and through various other industry standards and resources.

8. Acknowledgements and conclusion.

As chairman of the ANSI B77 AdHoc committee on Risk Assessment, I would like to thank the team members that have invested thoughtlessly and constructively their time, support, patience, resources and feedback over the past year in this development work. It has not been easy, and I have a feeling that we are not quite over the hump yet. This is a great document that everyone should be proud of. I would also like to thank Sid Roslund and Jon Mauch who seen the vision early, as did we, and provided the kick start necessary by nominating an AdHoc committee. We won't let you down.

In summary, the Risk Assessment AdHoc committee members are always available for discussion and openly welcome all constructive participation that can be offered.

Annex J
(Normative)

J. Safeguarding of passengers and personnel – risk assessment methodology

For new installations or relocations, a risk assessment shall be performed. The risk assessment shall take into account the stage of development, intended use of the Passenger Ropeway, anticipated skill and training of personnel, additional risk exposure and reasonably foreseeable events or misuse. A number of methodologies are available to do a risk assessment. Any method is acceptable which prescribes safeguarding equivalent to or more stringent than the requirements of this annex. The risk assessment process shall be instituted during the system planning/design phase and continue throughout the system construction, operation, and decommissioning. The risk assessment process shall emphasize the prevention of accidents by resolving hazards in a systematic manner as described below.

The hazard resolution process shall be initiated by defining the physical and functional characteristics of the Passenger Ropeway system to be analyzed. These characteristics shall be presented in terms of the people, procedures, facilities and equipment which are integrated to perform a specific operational task or function within a specific environment.

The hazards shall be identified. The techniques and methods used to identify the hazards shall include:

(1) Data from previous accidents or operating experience

(2) Expert opinion and hazard scenarios

(3) Checklists of potential hazards

(4) Previous hazard analyses

(5) Other analysis techniques as appropriate

All identified hazards shall be assessed in terms of the severity or consequence of the hazard and the probability of occurrence. This shall be accomplished in general accordance with the criteria outlined herein or equivalent.

Risk assessment estimates shall be used as the basis in the decision-making process to determine whether individual system or subsystem hazards shall be eliminated, mitigated, or accepted. Hazards shall be resolved through a design process that emphasizes the elimination of the hazard. For structures and foundations as defined in section x.1.1.6, an acceptable level of risk will be considered as being achieved if such structures and foundations are designed in accordance with section 1.3. For all other hazard resolution strategies, or safeguards, the following hierarchy of controls shall be employed, in order of effectiveness (most to least);

(1) Design by hazard elimination or substitution

(2) Engineered Safeguards

(3) Awareness means

(4) Administrative controls (Training and Procedures)

(5) Personal Protective Equipment

(6) Acceptance of the residual risk / Information for use concerning the residual risk

This process shall include full documentation of the hazard resolution activities. The effectiveness of the safeguards shall be monitored to determine that no new hazards are introduced. In addition, whenever substantive changes are made to the system, analyses shall be conducted to identify and resolve any new hazards introduced.

Where risk mitigation techniques and safeguarding methods are previously prescribed by various sections in this standard, the risk assessment shall serve as a method for determining suitable application according to the “hierarchy of controls” as well as functional safety circuit performance requirements as applicable. This method may be utilized to assess the applicability of a safeguard according to variable conditions or characteristics for a particular application.

This methodology is not meant to serve as a structural or component Failure Mode and Effects Analysis (FMEA), nor as a Fault Tree Analysis (FTA) for assessing the probability of structural or component failures within the passenger ropeway installation. FMEA and FTA are good methods for determining failure induced hazards, specifically in complex systems, and are very important to any complete hazard analysis. Failure modes identified through these processes shall be inherently designed out of the system utilizing prescriptive methods defined in this standard, through proven engineering methods, and through defining proper maintenance and testing cycles for components through the expected life of the equipment. In cases where an FMEA, FTA, or similar analysis predicts that a particular critical component failure is probable or imminent (inside of the expected lifespan of the equipment due to foreseeable neglect, inadequate maintenance cycles, or deficiencies in expected product quality or grade), then the method provided here may be used to provide further complementary risk mitigation measures.

J.1 Requirements

a) The risk assessment shall be performed by the **Designer or Manufacturer** at the time of initial Passenger Ropeway design to determine minimum safeguarding requirements and to develop an overall safety strategy. This assessment shall be revised and updated as the design process matures prior to installation of the Passenger Ropeway.

b) Additional risk assessments shall be performed by the **manufacturer and the owner** upon final installation and configuration, and again by the **owner** each time the operational configuration changes (I.e., maze and passenger loading configuration, ramp configuration, etc.) or a modification is made to the Passenger Ropeway. The owner shall maintain the documentation of the most recent risk assessment(s).

c) The first step of a risk assessment shall assume no **safeguards** are installed and include:

   - Determine the Limits of the Ropeway Installation per J.2.1
   - task and **hazard** identification per J.2.2
   - risk estimation per J.3

d) The next step of a risk assessment shall evaluate the level of risk and select suitable mitigation techniques based on the requirements established in table J.4 and table J.5

e) The final step of the risk assessment is to validate the safeguard selection by estimating residual risks as necessary, with the safeguards installed, per J.6

f) All processes above shall be clearly and completely documented.

g) Figure 1 provides a flowchart depicting the iterative process of risk assessment as outlined in this annex.

NOTE – This annex provides a composite risk assessment methodology based on similar methodologies utilized in other relevant safety-related standards.

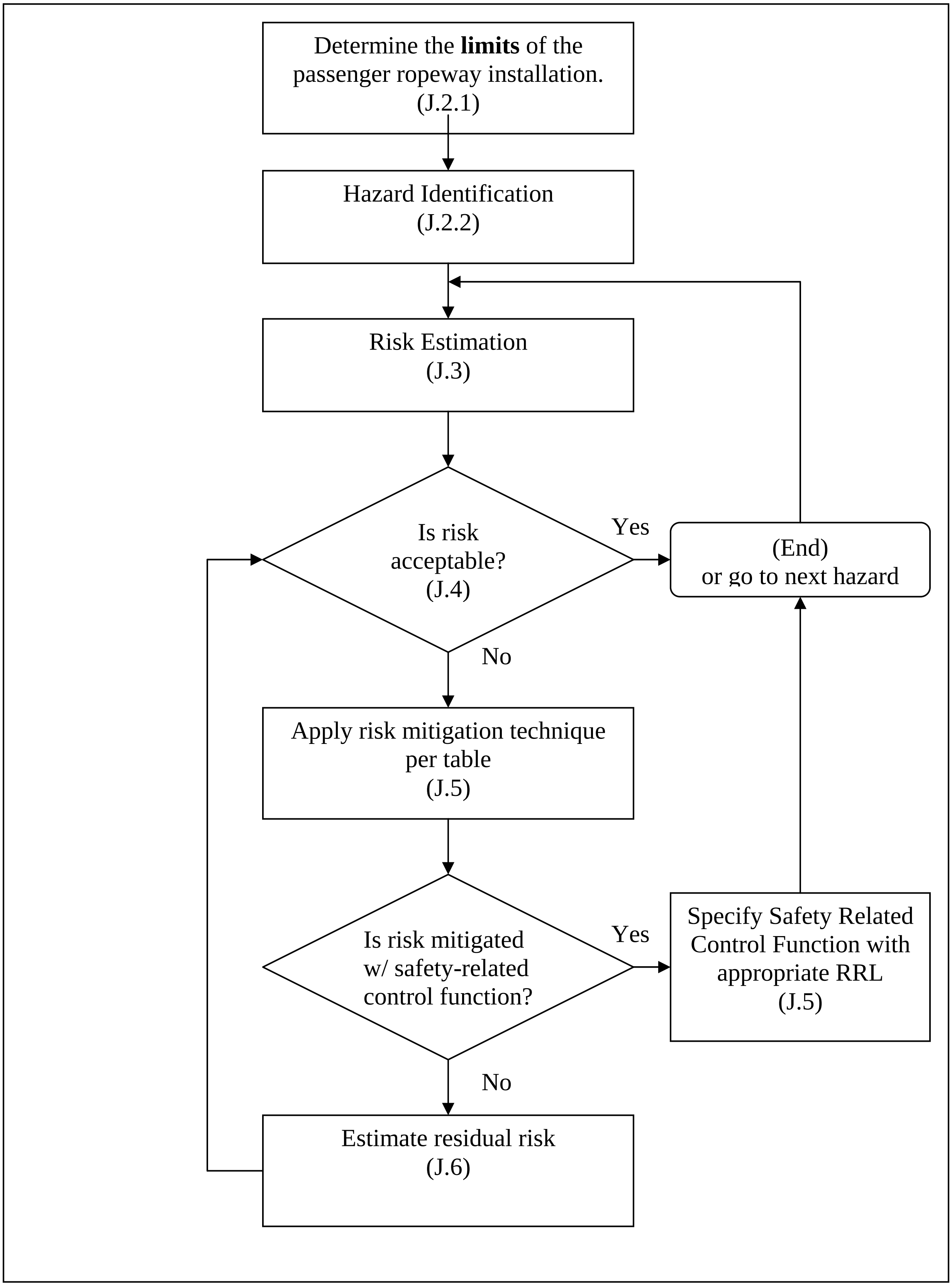

Figure 1 – Risk Assessment Flow Chart (General)

J.2 Determine the LIMITS of the ropeway and identify Hazards

J.2.1 Determine the **Limits** of the ropeway operation

Describe the application/process and a definition of the **limits associated with its intended use**; the risk assessment shall include a documented list of detailed specifications and operational parameters. It shall also include an elevation profile and plan view diagram showing the intended installation and operational configuration for all terminals, operator houses, operator stations, and line equipment. These elements will be used, in part, to set the basis for operational conditions that may be assumed for hazard identification and assessment. Note: Diagrams shall indicate the region of space describing the immediate interface to the passenger ropeway for which the scope of risk assessment shall be contained or defined.

J.2.2 Task and hazard identification

a) Hazard identification shall include at least the following three distinct categories:

   a. Passenger related use, foreseeable hazardous events and misuse.
   b. Operations related tasks, foreseeable hazardous events, and misuse.
   c. Maintenance related tasks, foreseeable hazardous events, and misuse.

b) Identify hazards associated with each task step, event, or instance of use for each of the categories list in (b) above, including those from reasonable foreseeable misuse. List them in the Hazard Description column in Table J.5.

   a. The hazard shall be qualified with respect to parts of body exposed to harm and the actual hazardous energy causing the harm.
   b. Hazardous energy sources shall be identified in this block for the purposes of specifying the proper energy control safeguard. [*See brackets in example below*].

Examples: (1) Passenger related (Detachable Chairlift):

Hazard I.D.	Event or Task	Description of Related Hazard
1	Passenger falls in load zone in front of following carrier	Concussions, fractures due to impact of following carrier, passenger legs, or skies into passenger while in pit area. **[Momentum of following carrier / Main drive motor]**
2	Passenger In-transit	Limb fractures, concussions, death due to passenger leaning too far forward and falling out of open carrier. **[Weight of Passenger, Gravity, distance of fall]**
3	Passenger In-transit	Limb fractures, concussions, or death to passengers due to carrier Impact with stalled carrier in decelerator section at 5 m/s. **[Main drive motor]**
4	Passenger In-transit	Limb fractures, concussions, or death due to passengers being ejected from carrier caused by deropement. **[Weight of carrier w/passengers, Gravity, Main drive motor]**

(2) Operations task related:

Hazard I.D.	Event or Task	Description of Related Hazard
1	Operator runs to pit area to assist improperly loaded passenger	Concussions, fractures due to impact of following carrier into operator.

J.3 Risk estimation

Risk estimation should be carried out for each hazard by determining the risk parameters in Figure 2. This is accomplished by combining the severity of harm (S) with the probability of occurrence of that harm, which is the combination of:

- the frequency and duration of the exposure of persons to the hazard (FD)
- the probability of hazardous event resulting from of the exposure (PE) and;
- the possibility to avoid or limit the severity of harm (AL).

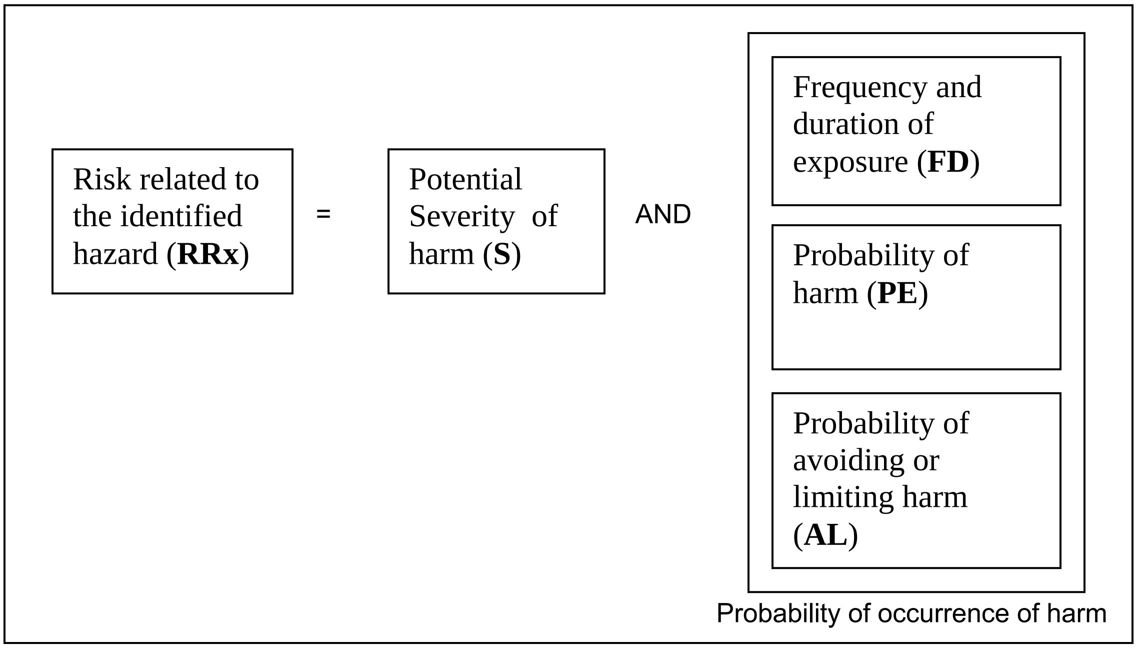

Figure 2 – Factors for Risk Estimation

The estimates of these parameters are entered into a form similar to Table J.3, and should normally be based on worst-case considerations for the hazard in order to provide the most conservative approach to the safeguard. Whenever in doubt, always choose the more conservative selection. However, in a situation where, for example, an irreversible injury is possible but at a significantly lower probability than a reversible one, then each severity level should have a separate line on the table. It may be the case that a different safeguard is implemented for each line. If one safeguard is implemented to cover both lines, then the highest Risk Reduction Level should be used.

Table J.3 – Example table / record of risk assessment data

Hazard I.D.	Event or Task (J.2.2)	Description of Related Hazard [w/ hazardous energy source] (J.2.2)	S (J.3.1)	FD (J.3.2)	PE (J.3.3)	AL (J.3.4)	PH = (FD+PE+AL)	RRL (Table J.6)	Recommended Risk Mitigation technique or safeguard
1									
2									

J.3.1 – Potential of hazard severity (S)

Risk estimation step 1: Select the hazard severity parameter based on worst-case potential hazard related to the event or task and enter this value into table J.3

Table J.3.1 – Severity of hazard (S) selection

Consequence	Severity
Major irreversible injury such as losing an eye or limb, and including death.	4
Irreversible injury such as a major broken limb(s) or losing finger(s)	3
Serious reversible injury requiring attention from a medical practitioner	2
Reversible injury requiring general first aid	1

This area reserved for supplementary recommendations and/or guidance.
/
/
/
/
/

J.3.2 – Frequency and duration of exposure to hazard (FD)

Risk estimation step 2: Select the frequency and duration of exposure to the hazard related to the event or task and enter the parameter in table J.3. For hazards in which exposure rate may be difficult to correlate, the frequency of exposure could be substituted with the frequency of demand on a safety function used to detect the exposure under worst case operating conditions. If in doubt between two selections, always choose the more conservative higher value.

Table J.3.2 – Frequency and duration of exposure to hazard (FD) selection

Hazard exposure occurs at a rate of:	Duration of each exposure is more than 10 minutes	Duration of each exposure is less than 10 minutes*1
Once per hour or more	5	5
Less than once per hour and up to once per day	5	4
Less than once per day and up to once every two weeks	4	3
Less than once every two weeks and up to once per year	3	2
Less than once per year	2	1

*1: For duration time, do not use the reduced value in the right column for hazard exposures when the exposure will always result in a hazardous event. I.e., Tower Deropement

This area reserved for supplementary recommendations and/or guidance.
/
/
/
/
/
/
/

J.3.3 – Probability of hazardous event (PE)

Risk estimation step 3: Select the probability of hazardous event related to the hazard exposure and enter the parameter into table J.3.

Table J.3.3 – Probability of hazardous event (PE) selection

Likelihood that the exposure will result in a hazardous event	Probability of Hazardous Event (PE)
Very high (>80% of exposures may lead to harm)	5
Likely (61-80% of exposures may lead to harm)	4
Possible (41-60% of exposures may lead to harm)	3
Rarely (21-40% of exposures may lead to harm)	2
Negligible (<21% of exposures may lead to harm)	1

This area reserved for supplementary recommendations and/or guidance.
/
/
/
/
/
/
/
/
/
/

J.3.4 – Probability of avoiding or limiting the severity of harm (AL)

Risk estimation step 4: Select the probability of avoiding or limiting severity of harm and enter the parameter into table J.3.

Table J.3.4 – Probability of avoiding or limiting the severity of harm (AL)

Probability of avoiding or limiting harm (AL)	
Impossible	5
Rarely	3
Probable	1

This area reserved for supplementary recommendations and/or guidance.
/
/
/
/
/
/
/
/
/
/
/
/
/

J.4 Risk Evaluation

Severity of the hazard (S) and probability of harm (PH) values recorded and calculated in Table J.5 are applied to the risk reduction decision matrix in table J.4 to determine the risk reduction level (**RRL**) for the associated hazard.

Table J.4 – Risk reduction decision matrix

Severity	Probability of harm **(PH)** = FD + PE + AL				
	(3-4)	(5-7)	(8-10)	(11-13)	(14-15)
4	RR2	RR2	RR2	RR3	RR3
3	Low	RR0	RR1	RR2	RR3
2	Low	Low	RR0	RR1	RR2
1	Low	Low	Low	RR0	RR1

This area reserved for supplementary recommendations and/or guidance.
/
/
/
/
/
/
/
/
/
/
/
/
/

J.5 – Safeguard Selection

With the Risk Reduction Level (RRL) now determined, utilize Table J.5 to determine the appropriate risk reduction technique or engineered safeguard. Note: An attempt should always be made to eliminate the hazard through redesign or substitution, regardless of the RRL. If the level of risk is at RRL=Low to begin with, at least some type of mitigation, even if minor, should be made if possible. At least one complete pass of risk mitigation should be made for each identified hazard. See table J.5.3 for an example showing all columns completed.

This area reserved for supplementary recommendations and/or guidance.
/
/
/
/
/
/
/
/
/

Table J.5.1 – Risk reduction and Safeguard Selection Guide

<table>
<tr><th>Risk Reduction Category</th><th>Safeguard Performance</th><th>Hierarchy Of Risk Reduction Measure (Effectiveness Most To Least)</th></tr>
<tr><td>RR3</td><td>Rigorous attempt required:
[Elimination] Risk reduction shall be accomplished by hazard elimination or hazard substitution which does not create an equal or greater hazard. Where hazard elimination or substitution is not possible;

Required alternative:
[Engineered Safeguards] preventing access to the hazard or causing the hazard to cease. Functional safety circuits, if applied, shall meet the requirements of **RR3**, per Table J.8.</td><td rowspan="5">**Elimination or substitution:**
• Eliminate human interaction with hazard
• Automate hazardous process to substitute lower risk for higher risk.
• Increase clearances

Engineered Safeguards:
• Fixed barriers
• Interlocked barriers.
• Mechanical hard stops.
• Anti-collision function.
• Rope position detection function.
• Over-speed detection function.
• Calculated safety distances shall be validated for all engineered safeguards as applicable

Awareness Means:
• Start alarms.
• Operator interface warnings.
• Signs.
• Painted Floor boundary
• Beepers.
• Horns.
• Labels.

Administrative Controls:
• Job safety procedures.
• Safety equipment inspections.
• Training.
• Lockout.
• Information for Use

PPE / Personal Protective Equipment:
• Safety glasses.
• Ear plugs.
• Face shields.
• Gloves.</td></tr>
<tr><td>RR2</td><td>Attempt:
[Elimination]. Where hazard elimination or substitution is not possible or impracticable;

Required:
[Engineered Safeguards] preventing access to the hazard or causing the hazard to cease. Functional safety circuits, if applied, shall meet the requirements of **RR2**, per Table J.8.</td></tr>
<tr><td>RR1</td><td>Attempt:
[Elimination]. Where hazard elimination or substitution is not possible or impracticable;

Required:
[Engineered Safeguards] preventing access to the hazard or causing the hazard to cease. Functional safety circuits, if applied, shall meet the requirements of **RR1**, per Table J.8.</td></tr>
<tr><td>RR0</td><td>Attempt:
[Elimination]. Where hazard elimination or substitution is not possible or impracticable;

Required:
[Awareness means]
And/Or
[Administrative Controls]
And/Or
[PPE]

Functional safety circuits, if applied, shall meet the requirements of **RR0**, per Table J.8.</td></tr>
<tr><td>LOW</td><td>Required:
[Awareness means]
And/Or
[Administrative Controls]
And/Or
[PPE]</td></tr>
</table>

Table J.5.2 - Defined relationship between relevant functional safety standards.

Risk Reduction Level (RRL) - ANSI B77.1	Safety Integrity Level (SIL) - IEC 62061	Performance Level (PL) - ISO 13849-1	Average probability of dangerous failure per hour [1/h]	Reserved for future information
RR3	3	PLe	$\geq 10^{-8}$ to $< 10^{-7}$	
RR2	2	PLd	$\geq 10^{-7}$ to $< 10^{-6}$	
RR1	1	PLc	$\geq 10^{-6}$ to $< 3 \times 10^{-6}$	
RR0	1	PLb	$\geq 3 \times 10^{-6}$ to $< 10^{-5}$	
Low	N/A	PLa	$\geq 10^{-5}$ to $< 10^{-4}$	
Correlation between Safety Integrity Level (SIL) and Performance Level (PL) per ISO 13849-1:2006 Table 4.				

This area reserved for supplementary recommendations and/or guidance.
/
/ - qualitative descriptions of relevant SILs and PLs with respect to structure (designated architecture), fault tolerance, diagnostic coverage, common cause failure, etc. to provide a generalized description to the user.
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/

Table J.5.3 – Example of the identification and risk estimation for a single event/hazard combination

Hazard I.D.	Event or Task (J.2.2)	Description of Related Hazard [w/ hazardous energy source] (J.2.2)	S (J.3.1)	FD (J.3.2)	PE (J.3.3)	AL (J.3.4)	PH = (FD+PE+AL)	RRL (J.4)	Recommended Risk Mitigation technique or safeguard (J.5)
1	Passenger In-transit	Limb fractures, concussions, or death to passengers due to carrier Impact with stalled carrier in decelerator section at 5 m/s. **[Main drive motor]**	4	4	5	5	14	RR3	**[Engineered Safeguard]** Anti-collision monitoring system / safety-related control function (SIL 3 or PLe per J.6)
2									

Note: The description under (Recommended risk mitigation technique or safeguard) is meant to serve as a safety function definition and not necessarily a safety requirements specification (SRS).

J.6 – Evaluating residual risk

Once a risk mitigation technique or engineered safeguard are applied, it is necessary to assess the residual risk that may remain.

When a safety-related control function has been defined, and designed such that it's correct functioning eliminate exposure to the hazard, and the safety function has been designed to a correlating SIL or PL (table J.5.2), then the risk may be considered to be effectively reduced to a tolerable level.

If the mitigation technique is other than an engineered safeguard, or, if the engineered safeguard does not effectively control all factors of the hazard, then it will be necessary to assess **residual risk** that may be remaining.

J.6.1 Assessing residual risk

The first step in calculating residual risk is to generate a further set of columns for S, FD, PE, AL, and a new result for PH and RRL. The risk parameters should now be re-assessed with the mitigation technique employed. This technique should have some effect on S, FD, PE, or AL in some combination such that the overall risk reduction level (RRL) will have been decreased.

This new value for RRL is the **residual risk** that remains. This residual risk should be re-evaluated and further mitigation techniques employed until the risk is considered acceptable.

Acceptable risk shall be a risk level at which further risk reduction will not result in significant reduction in risk; or additional expenditure will not result in significant advantages of increased safety. Collaboration should be shared between the ropeway system manufacturer, or entity conducting the risk assessment and the owner, as these entities may have different levels of acceptable risk.

When the hazard mitigation is complete, the conditions shall be re-assessed qualitatively to ensure that no new hazards have been created.

This area reserved for supplementary recommendations and/or guidance.
/
/
/
/
/
/
/
/

J. Definitions ……..Section still in Progress

Failure: termination of the ability to perform an intended function.

Hazard: A potential source of harm

PPE: Personal protective equipment (I.e. safety glasses, safety shoes, hearing protection)

Protective Measure: Measure intended to achieve risk reduction. (I.e. inherently safe design, safeguarding, complementary measures, PPE, safe working procedures, training, supervision, information for use)

Risk(1): combination of the severity of harm and the probability of occurrence of that harm

Risk (2): A measure of the severity and likelihood of an accident.

Risk Analysis: combination of the specification of the limits of machine, hazard identification and *risk estimation*

Risk Assessment: overall documented process comprising a *risk analysis*, application of *protective measures*, and *risk evaluation*

Risk Evaluation: judgment, on the basis of risk analysis, of whether the risk reduction objectives have been achieved

Residual Risk: The element of risk remaining relative to a hazard after a risk reduction technique or safeguard has been applied.

Interlock: An arrangement of control elements so interconnected that their operations must succeed each other in proper sequence.

Safeguard: A barrier guard, device, or safety-related control function designed for the protection of personnel or passengers.

Safe State: System state that is deemed acceptable by the hazard resolution process.

Safety: Freedom from unacceptable risk.

Subsystem: A major functional subassembly or grouping of items or equipment that is essential to operational completeness of a system.

System: A composite of people, procedures, facilities, and/or equipment that are integrated to perform a specific operational task or function within a specific environment.