Exhibit I: Traffic Safety and Security

_____/_____

Signature

Exhibit I: Traffic Safety and Security

Table of Contents

_____/_____

Signature

Exhibit I: Traffic Safety and Security

1 GENERAL

Id		Requirement	Referring to
I:1.a	I	The purpose of this document is to describe the requirements regarding the traffic safety taking into account different aspects for this contract.	
I:1.b	I	All documents regarding traffic safety, IT safety and cyber and physical security should be derived from an overall contract quality plan (CQP). Documents that is derived from the CQP must be sent to NT for acceptance. All further changes to the documents shall be accepted by NT.	

_____/_____

Signature

2 TRAFFIC SAFETY

Id		Requirement	Referring to
I:2.a	I	Traffic safety in this context means all safety related aspects relevant for design, technical solutions, and documentation for the trainset with risk elements from: • Train operation including maintenance and operation • Construction and system integrity • Security on on-board- and system protection including IT security • Onboard work environment • Environment interfaces towards traffic safety • Emergency preparedness	
I:2.b	I	For NT to be able to follow and participate in the safety process it is important that a proven process is followed and that important information from this process is provided through: • Review and acceptance of safety process documents • Regular safety follow-up meetings • Participation in authority meetings	
I:2.c	I	The traffic safety activities shall be documented and part of the contract quality plan, see Exhibit I and Appendix I-2 (clause 1.3.1)	Exhibit I, Appendix I-2

2.1 Traffic Safety Plan

Id		Requirement	Referring to
I:2.1.a	K	The Contractor shall develop and establish a traffic safety plan according to EN50126-1:2017 chapter 7.3.2.3, “Safety Plan”. The safety plan shall include the relationship to relevant involved stakeholders throughout the life cycle of the system under the contractor’s responsibility.	EN50126-1:2017
I:2.1.b	K	The Contractor shall deliver a preliminary safety plan with the tender and within eight (8) weeks from Effective Date prepare and submit a first version of a traffic safety plan for the Work under the Contract to NT for acceptance. The safety plan shall as a minimum comply with I:2.1.e .	I:2.1.e

Id		Requirement	Referring to
I:2.1.c	K	The plan shall as a minimum follow the principal shown in figure 1 to ensure traceability from all risk- and relevant RAM analyses throughout the process to final user documentation.	

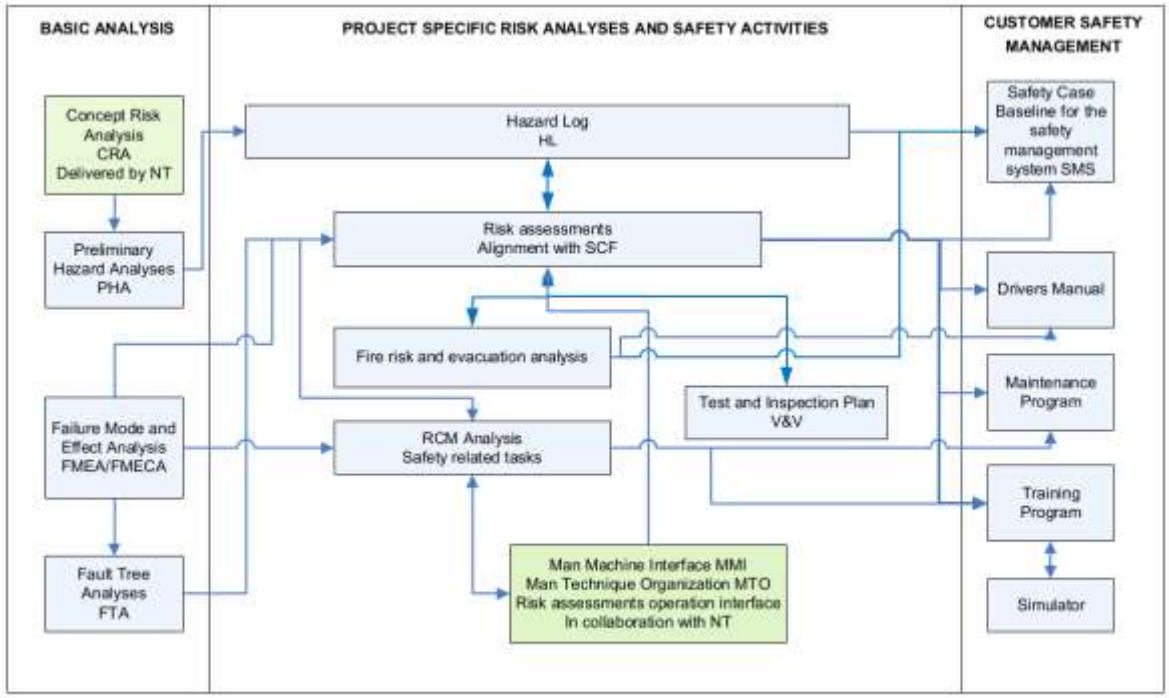

Figure 1 Principle of management of risk assessments and safety documentation

I:2.1.d	K	The preliminary Traffic safety plan and all changes shall be accepted by NT.	

/

Signature

Id		Requirement	Referring to
I:2.1.e	E	The Traffic safety plan shall contain the approach to the safety work to be addressed during the project execution. Aligned with the requirements in EN50126-1:2017 chapter 7.3.2.3, the plan should at least include: a) the scope of the plan; b) an overview of governing documents, including relevant laws and regulations, relevant contractual requirements, specifications, standards, and a complete list of deviations. Risk assessments shall be documented for deviations; c) a description of the organization of the traffic safety work including responsibilities, competence, authority and duties; d) relevant interfaces with the RAM- and quality plan shall be specified; e) the policy and strategy for achieving an acceptable safety level; f) a plan of the safety activities; g) the underlying system life cycle as well as the safety analysis, engineering processes and relationship with assessment to be applied during the life cycle, including: – ensuring an appropriate degree of personnel independence in tasks where independence is required; – the approach for hazard identification and preliminary analysis; – risk assessment and on-going risk management and hazard log; – risk acceptance criteria; – alignment of safety critical functions (ref. ch. 2.2) to review the effectiveness of risk reduction measures in design, maintenance and operation; – the establishment and on-going review of the adequacy of the safety requirements; – a process for verification and validation; – achievement of compliance of the management process with the safety plan (e.g. confirmed via audits); h) a plan of all safety-related documentation deliverables from the life cycle phases; i) a process for the identification of safety-related maintenance; j) a process for management and handover of the hazard log; k) description of any constraints and assumptions made in the plan; l) management of sub-contractors including requirements; m) a plan for safety audits; n) a process to prepare the safety case. *The Tenderer shall demonstrate compliance by delivering a preliminary Traffic Safety plan.*	EN50126-1:2017

2.2 Risk Assessment Process

Id		Requirement	Referring to
I:2.2.a	M	The risk assessment process shall comply with the EU regulation 402/2013 Common safety method for risk evaluation and assessment, CSM RA as referred to in Directive 2004/49/EC, Railway safety directive.	EU regulation 402/2013 Common safety method for risk evaluation and assessment
I:2.2.b	K	The risk assessments shall be based on EN 50126-1 risk-based approach, risk reduction strategy and risk assessments.	EN 50126-1
I:2.2.c	K	All basic analyses for risk assessments, e.g. failure mode, effect (and criticality) analysis/FME(C)A, fault tree analysis/FTA, etc. to be presented to NT upon request.	
I:2.2.d	I	NT has performed a concept risk assessment to identify typical risks related to the design and operation of the conceptual trainset based on experience from operation of similar existing trainsets on the Norwegian railway network. The concept risk assessment will be submitted to the contractor after contract award and the contractor is obliged to include relevant risks in their hazard list and preliminary risk assessments.	
I:2.2.e	E	The safety critical functions, SCFs, are supplied by NT in document NOR0000463 “Generic Safety Critical Functions”, Exhibit I, Appendix I-1. The list of generic SCFs may be expanded following input from the Contractor. The safety critical functions shall be aligned with the results of the risk analysis to assess the effectivity of the implemented risk reducing measures and to ensure the alignment to the NT safety management system. *The Tenderer shall describe how the results of the risk assessments are identified to the respective SCF and transferred to the user documentation, e.g. maintenance program, drivers manual and drivers and maintainers training programs. There shall be full traceability between the decisions in the risk assessments and the safety related measures implemented in the user documentation.*	Document NOR0000463 “Generic Safety Critical Functions”, Exhibit I, Appendix I-1

2.3 Generic Safety Critical Functions (SCFs)

Id		Requirement	Referring to
I:2.3.a	I	The Trainset shall be designed with effective measures (barriers) in a way that protect a SCF and ensures that no single failure can lead to a railway accident. Fulfilment of this requirement should be documented as part of a risk analysis report, hazard log or in a separate report. Measures (barriers) implemented to reduce the probability of single failures leading to hazards and measures (barriers) that reduce the consequences of accidents should be identified, documented and communicated to NT. This implies that sufficient technical, operational, organizational or other planned measures should be implemented for the purpose to prevent an initial fault from developing into a critical operational or accident condition. If several barriers are required, the interdependency between these barriers should be demonstrated.	
I:2.3.b	K	The Contractor shall enter the measures to safeguard the SCFs in the “Technical or operational measures to control the SCF” column in NOR0000463”. NT accepts that the Tenderer either uses descriptions or references to the technical specifications and RAM analysis to be delivered with the Tenderer's Traffic safety plan.	Document NOR0000463

2.4 Preliminary Hazard Analysis, PHA

Id		Requirement	Referring to
I:2.4.a	K	The Contractor shall within three (3) months from Effective Date prepare and submit a PHA report.	
I:2.4.b	E	The main purpose of the PHA is to: • Identify all potential hazards and accidental events that may lead to an accident; • Rank the identified accidental events according to their severity; • Identify required hazard controls and follow-up actions; • Form a basis for the establishment of the Hazard Log. *The Tenderer shall demonstrate how the hazards are identified and describe the process of determine the severity and the follow up actions to be transferred to the hazard log.*	

2.5 Hazard log

Id		Requirement	Referring to
I:2.5.a	K	A Hazard log shall be established as the basis for on-going risk management for safety and shall be based on the requirements in EN50126 -1. The Hazard log shall be established in RAMS phase 3 including hazards identified in the PHA and relevant hazards from the NT Concept Risk Analysis. From this point the Hazard log process shall assemble all risks and hazards identified in all RAMS phase activities and be updated accordingly.	EN50126 -1

Id		Requirement	Referring to
I:2.5.b	E	The Hazard Log shall be aligned with the requirements in EN50126 and include the following: • The purpose of the hazard log; • Each hazard, entities responsible for managing the hazard, and the contributing functions or components; • Likely consequences and frequencies of the sequence of events associated with each hazard, when applicable; • The risk arising from each hazard (in quantitative or qualitative terms), where appropriate; • Risk acceptance principles selected and in case of explicit risk estimation also reference to the risk acceptance criteria to demonstrate the acceptability of the risk control related to the hazards; • For each hazard; the measures taken to reduce risks to a tolerable level or to remove the risks; • The process to identify hazards throughout the project RAMS phases; • The process or procedure to close a hazard; • Exported safety constraints; e.g. SRR's (safety related requirements), SRAC's (safety related application conditions) and SCF's (safety critical functions). *The Tenderer shall describe the content of the hazard log, the process of entering and close out of hazards, responsibilities and if risk assessments are included in the hazard log the method approach shall be described or referred to.*	EN50126

2.6 Safety Case

Id		Requirement	Referring to
I:2.6.a	K	The safety case shall be assembled according to EN 50126-1 chapter 8. The preliminary version of the safety case shall be submitted 3 months before first test-run on Norwegian tracks and the final safety case shall be submitted four (6) months before APIS/APIM.	EN 50126-1 chapter 8

Id		Requirement	Referring to
I:2.6.b	E	The main requirements to the safety case are: • Identification of all traffic safety aspects and risk elements covered by the Safety report; • Full description of the operation of the Trainset with emphasize on the traffic safety aspects (including relevant drawings and system description); • Description of measures taken in order to reduce the possibility for and/or the consequences of accidents (i.e. “safe” functions, safety margins, passive and active safety devices, automate, redundancy and diversification); • Description of new technology and all related traffic safety aspects; • Traffic safety evaluation; • Systematic evaluation of all technical sub-systems and causal relation influencing traffic safety, such as resistance against derailing, operation restrictions, maintenance intervals, design philosophy and running characteristics; • Identification of interface and adjacent systems influencing traffic safety, as well as specification of conditions and limitations valid for how the Trainset and the surrounding environment are influencing each other; • A clear and unambiguous conclusion.	

3 IT SAFETY

Id		Requirement	Referring to
I:3.a	K	Functional safety integrity requirements for electronic systems (E/E/EP) shall be apportioned and allocated to relevant safety integrity (SIL) level according to EN50126-2.	EN50126-2
I:3.b	K	Development, deployment, and maintenance of software included in systems/sub-systems with functional safety and SIL requirements shall comply with EN50128 or EN50657.	EN50128, EN50657

_____/_____

Signature

4 CYBER AND PHYSICAL SECURITY

Id		Requirement	Referring to
I:4.a	I	Train control systems have evolved in recent years increasing their connectivity and offering new functionalities. Remote train status monitoring, live CCTV video streaming from trains, or passenger Wi-Fi services provide an added value to the product and passengers. However, these new features have also increased the attack vectors the trains may be exposed to.	

4.1 Cyber Security Concept

Id		Requirement	Referring to
I:4.1.a	K	The cyber security concept shall be based on IEC 62443 series “Industrial communication networks - Network and system security” or equivalent. The Contractor shall within 15 weeks from Effective Date prepare and submit a first version of a cyber security concept report to NT for acceptance including a plan describing vulnerability and risk assessments to be implemented.	IEC 62443
I:4.1.b	E	The cyber security concept should include but not limited to: • Overall security for the Trainset; • Ensure sustainable development of security on the train; • Describe a cyber security design and architecture include, but not limited to: o Zones, conduits (connections); o Identification of attack vectors (threats); o Physical security/HW and network; o Wayside interfaces; o Firewalls; o Network segmentation; o SW updates; o Communication buses; o Risk assessment; • Risk assessment and risk acceptance criteria; • Security countermeasures. *The Tenderer shall describe the approach to comply with a sustainable cyber security concept.*	

4.2 Physical Security Concept

Id		Requirement	Referring to
I:4.2.a	K	The Contractor shall within 15 weeks from Effective Date prepare and submit a first version of a physical security concept report to NT for acceptance. The physical security concept shall describe implementation of system- and layout design to prevent violent acts, vandalism, and threats/terrorism.	