Trust-Indicator

Risk Management

Group member

u7588748	Lingxiu Cai
u7504537	Tony Chen
u7529732	Song Han
u7531066	Vidhu Chaudhary
u7342064	Yifang Meng
u7545864	Zhaoyun Zhang

1. Introduction

Risk management plays a very important role in project management. It identifies, evaluates, and controls any known and potential risks in the process of project development.

In this project, we will design a set of risk identification and management methods to help project managers or R&D engineers in risk management.

2. Risk management methods

2.1 Classification of hazards and risk assessment criteria

In order to identify and manage risks better, firstly, we classify the hazards that risks may bring. We divide the severity of hazards into 5 different levels, from level S1 to level S5. Different levels represent different degrees of severity. Similarly, we divide the probability of hazard occurrence into 6 levels.

1) Classification of the severity of hazards

Table 2.1 Classification of the severity of hazards

Classification of hazard severity		Classification criteria
S1	Negligible	Inconvenience or temporary discomfort.
S2	Minor	Temporary trauma or injury resulting in no occupational medical intervention.
S3	Serious	May cause trauma or injury requiring occupational medical intervention.
S4	Critical	May cause permanent damage or life-threatening trauma.
S5	Catastrophic	May cause the user’s death.

If the severity of the injury is between two classifications and cannot be accurately estimated, risk analysis should be performed with the more serious classification as much as possible.

2) Classification of the occurrence probability of hazards

Table 2.2 Classification of the occurrence probability of hazards

Classification of occurrence probability of hazards		Event frequency (product per year)
P6	Frequent	> 1
P5	Probable	$1 \sim 10^{-1}$
P4	Occasional	$10^{-1} \sim 10^{-2}$
P3	Remote	$10^{-2} \sim 10^{-4}$

P2	Unlikely	$10^{-4} \sim 10^{-6}$
P1	Incredible	$< 10^{-6}$

If the occurrence probability of hazards is between two classifications and cannot be accurately estimated, the risk analysis should be performed on the stratification with a higher probability as much as possible.

3) Risk assessment criteria

Table 2.3 Risk assessment criteria

Occurrence probability of hazards	**Severity of hazards**				
	S1	**S2**	**S3**	**S4**	**S5**
P6 - Frequent	NAC	NAC	NAC	NAC	NAC
P5 - Probable	ALARP	NAC	NAC	NAC	NAC
P4 - Occasional	ALARP	ALARP	NAC	NAC	NAC
P3 - Remote	ACC	ALARP	ALARP	NAC	NAC
P2 - Unlikely	ACC	ACC	ALARP	ALARP	ALARP
P1 - Incredible	ACC	ACC	ACC	ACC	ACC

In the table above, NAC stands for unacceptable, ACC stands for acceptable and ALARP stands for as low as reasonably practicable.

After taking risk control measures, all residual risks must be controlled to an acceptable level. That is to say, all remaining risks at NAC level are not allowed after measures are taken. On the other hand, the number of risks at ALARP level must be less than 5.

2.2 Risk management methods

1) Risk identification

In order to control and manage risks, we should identify the risks and hazards first. We have identified and estimated the risks and hazards for stage one, H1. Below is the initial hazard analysis form we designed (Table 2.4). In this table, we should use system thinking method to analyse and identify all known and potential risks and hazards of the project and the product, including identifying and analysing the hazard type, source, foreseeable sequence of events, and under what circumstances these hazards will occur, what damage or consequences will be caused, and what risk control plans and measures they plan to use.

Table 2.4 Initial Hazard Analysis Form

Hazard Identification	Hazard Type	Hazard (Source)	Foreseeable Sequence of Events	Hazardous Situation	Consequence or Damage	Initial Risk Control Plan
H1.1	Ethical hazard	Detection Decision	1. Detection algorithms may have false positives or omissions 2. There is a potential for malicious use of the technique, such as the deliberate falsification of real images in order to target a person or organization.	Unethical outcomes from detection.	Loss of reputation, legal disputes or financial losses	1.Provide mechanisms for users to raise objections and fix buggy flags. Ensure that systems are adequately tested and validated to minimize errors 2. monitoring user behavior and enforcing strict usage policies and restrictions.
H1.2	Cyberattack	External Threat Actors	Malicious entity tries to breach the system.	Unauthorized system access.	Data breach, service disruption.	Implement robust cybersecurity measures, regular vulnerability assessments, and penetration testing.
H1.3	Privacy	External Threat Actors	User data is mishandled or stored without proper security.	Privacy violations.	Identity theft, loss of trust, legal penalties.	Strict data handling policies, end-to-end encryption, and clear user consent mechanisms.
H1.4	Copyright	Content Uploads	Users upload copyrighted content without permissions.	Copyright infringements.	Legal disputes, financial penalties.	Automated content detection mechanisms, clear terms of service regarding uploads, and prompt response to takedown notices.
H1.5	Design and update	System Development	Poorly designed user interface or updates that introduce issues.	Usability and functionality issues.	Poor user experience, decrease in user trust.	Regular user testing, feedback loops, and phased rollouts for updates.

H1.6	Performance	System Infrastructure	High traffic or complex queries slow down the system.	Slow or non-responsive platform.	User dissatisfaction, potential loss of users.	Scalable infrastructure, regular performance testing, and optimization techniques.

Next, we need to formulate risk control measures and methods for verifying and confirming that the risks have been reduced or eliminated for each identified risk. At the same time, we need to evaluate the severity, probability, and risk level of hazards after risk control, and at the same time, identify whether new risks have been introduced. Table 2.5 is a risk and risk control measures evaluation form we design. We can intuitively know what kind of risk control measures we should conduct, and what effects will the measures achieve.

Table 2.5 Risk and risk control measures evaluation form

Hazard Identification	**Hazard Type**	**Risk Estimation**			**Risk Control Measures**	**Validation results**	**Risk Level after controlled**			**New Risks**
		Severity	**Probability**	**Risk Level**			**Severity**	**Probability**	**Risk Level**	
H1.1	Ethical hazard	S3	P3	ALARP	The EMC related design should follow the relevant requirements in industrial standard YY 0505-2012	Product Registration Inspection Report	S3	P1	ACC	None
H1.2	Cyberattack	S4	P5	NAC	In accordance with the game Terms of Services (ToS)	Improved detection and prevention of unauthorized toolkits and cheating. Prompt investigation and enforcement the penalties	S3	P2	ALARP	Authorization of Terms of conditions and services
H1.3	Privacy	S5	P2	ALARP	Various jurisdictions have regulations concerning malware, including the Computer Fraud and Abuse Act in the U.S. and the European Union's Directive	Decreased incidence of malware-infect software. Prompt mitigation of vulnerabilities and security threats	S5	P1	ACC	Invalid

					on Security of Network and Information Systems (NIS Directive).					
H1.4	Copyright	S3	P5	NAC	The enforcement of anti-cheating measures falls under the jurisdiction of the game's Terms of Service. The Federal Trade Commission (FTC) in the U.S. also enforces laws against deceptive practices, which could apply to cheating in online games.	Increase player satisfaction. Enhanced trust and retention and built up a well game community.	S3	P2	ALARP	Invalid
H1.5	Design and update	S2	P2	ACC	No specific laws or regularities to support but accordance with the best practices in software development to ensure compatibility and provide technical support.	Decreased occurrence of compatibility issues and crashes. Improved overall game stability.	S2	P1	ACC	New system compatibility and stability
H1.6	Performance	S2	P3	ALARP	Each online service's Terms of Service are considered a legal agreement. Failure to comply can result in civil litigation. In many jurisdictions, digital contracts such as these are legally enforceable under laws like the U.S.'s Uniform Electronic Transactions Act (UETA) and the European Union's eIDAS regulation.	Increased awareness and adherence to Terms of Services. Reduced violations and improved player conduct	S2	P2	ACC	Invalid

As shown in Table 2.5, the risk of each hazard has been reduced to an acceptable or reduced level.

The following tables (Tables 2.6 and 2.7) are the risk assessments before and after taking risk control measures, risk and hazards in the stage one is highlighted red. The comparison shows that after the risk control measures are taken, the overall residual risk of the equipment after the design change has been reduced to an acceptable range.

Table 2.6 Risk assessment before taking risk control measures

Risk assessment		Severity of hazards				
		Negligible	**Minor**	**Serious**	**Critical**	**Catastrophic**
Occurrence probability of hazards	**P6 (Frequent)**					
	P5 (Probable)			1(**H1.4**)	5 （**H1.2**, H2.1， H2.2， H2.3， H2.4）	
	P4 (Occasional)				1 （H3.1）	
	P3 (Remote)		16 （**H1.6**, H3.4， H3.5， H3.6， H3.7， H3.8， H4.1， H4.3， H4.4， H4.5， H4.6， H4.8， H4.9， H5.1， H5.2， H6， H7）	4 （**H1.1**, H1.4， H3.2， H3.3）		
	P2 (Unlikely)		1(**H1.5**)		2 （H4.2， H4.7）	1(**H1.3**)
	P1 (Incredible)					

Table 2.7 Risk assessment after taking risk control measures

Risk Assessment		Severity of hazards				
		Negligible	Minor	Serious	Critical	Catastrophic
Occurrence probability of hazards	P6 (Frequent)					
	P5 (Probable)					
	P4 (Occasional)					
	P3 (Remote)					
	P2 (Unlikely)		1 (H1.6)	2 (H1.4, H1.2)		
	P1 (Incredible)		17 （H1.5, H3.4， H3.5， H3.6， H3.7， H3.8， H4.1， H4.3， H4.4， H4.5， H4.6， H4.8， H4.9， H5.1， H5.2， H6， H7）	5 （H1.1， H1.4， H3.2， H3.3， ）	7 (H2.1， H2.2， H2.3， H2.4， H3.1， H4.2， H4.7）	1 (H1.3)