Security Analysis results

1 Context identification

The purpose of this section is to identify the parts of the system that is relevant for our analysis, and to establish a framework for the analysis.

1.1 Target of Evaluation

Type:	Table
Name:	Target of Evaluation
Short description:	What to analyse and for whom
Concern:	Target of evaluation
Full description:	The security analyse is performed on behalf of the designers of the blind date system. They want to find and remove as many security hazards as possible at an early stage. By focusing on security from the start, the final system will probably be safer. Neither the Trafikanten nor the SMS module are analysed since they are external systems.

Table 1: Target Of Evaluation Table

Category	Value
Target	Communication between the client and the blind date system.
Client	Blind Date Designers
Service/Function	Registering customers, joining events, making events and notifying customers. Both Trafikanten and SMS/position service are external parts, and they will therefore not be analysed, though we do consider how their interface may affect the system.
Quality aspects	The internal functionality of the BD system and the availability of the BD system will be addressed in the analysis.

1.2 Value Definition Table

Type:	Table
Name:	Value Definition Table
Short description:	Values and definitions
Concern:	Target of evaluation
Full description:	Describes the values and definitions used through the analysis. The definitions given here are used to judge the risks and determine which risks must be addressed and which ones are less severe.

Table 2: Value Definition Table

Type	Domain	Allowed values	Description
Asset	NOK	Very Low, Low, Medium, High, Very High	Very Low: Less than 10 NOK (1 SMS) Low: 10 - 500 NOK (1 event) Medium: 500 - 5000 NOK (Trafikanten, customer) High: 5000 - 500000 NOK (registers) Very High: Above 500000 NOK (SMS system)
Frequency		Unlikely, Rare, Possible, Likely, Certain	Unlikely: Less than once per 3 years Rare: Less than once a year Possible: 2- 5 times a year Likely: About once a month Certain: 2-5 times a month
Consequence		Insignificant, Minor, Moderate, Major, Catastrophic	Insignificant: No impact on business, minor delays Minor: Loss of profits Moderate: Loss of customer Major: Loss of market. Catastrofic: Out of business
Risk value		Low, Moderate, Major, Critical	Low: Low risk Moderate Some risk, should be aware of Major Serious risk, should be fixed Critical Very serious risk, must be fixed before release

1.3 Risk Matrix

Type:	Table
Name:	Risk Matrix
Short description:	Risk matrix
Concern:	Target of evaluation
Full description:	The matrix defines how serious risks with a given frequency and consequence should be considered.

Table 3: Risk Matrix

Frequency	Insignificant	Minor	Moderate	Major	Catastrofic
Certain	Moderate	Major	Major	Critical	Critical
Likely	Low	Moderate	Moderate	Critical	Critical
Possible	Low	Low	Moderate	Major	Major
Rare	Low	Low	Low	Major	Major
Unlikely	Low	Low	Low	Moderate	Major

1.4 Asset Table

Type:	Table
Name:	Asset Table
Short description:	Assets for the client
Concern:	Assets
Full description:	Descriptions of the things that have value for the client. The stated values refer to the value definition table in section 1.2.

Table 4: Asset Table

Asset ID	Description	Category	Value
Customer Trust	Trust from customer	Other	High
Reputation	Company reputation	Organisational	Very High
Customer register	The database of the registered customers	Information	Very High
Event register	The database of the registered events	Information	High
System availability	The control system is up and running	Software	Very High
Physical	The equipment which the system uses	Physical	High

1.5 Risk Evaluation Criteria Table

Type:	Table
Name:	Risk Evaluation Criteria Table
Short description:	Risk Criterias
Concern:	Risk evaluation criteria
Full description:	Which risk levels an asset can accept

Table 5: Risk Evaluation Criteria Table

Criteria ID	Criteria	Description	Applied for assets
C1	risk value < Major	OK if value < Major	Reputation
C2	risk value < Major	OK if value < Major	Customer register
C3	risk value < Major	OK if value < Major	Event register
C5	risk value < Major	OK if value < Major	System availability
C6	risk value < Major	OK if value < Major	Physical

2 Risk identification

2.1 HazOp Table

Type: Table
Name: HazOp Table
Short description: Hazards and operations
Concern: Threats
Full description: This table describes potential threats to the Blind date system, as identified through HazOp sessions.

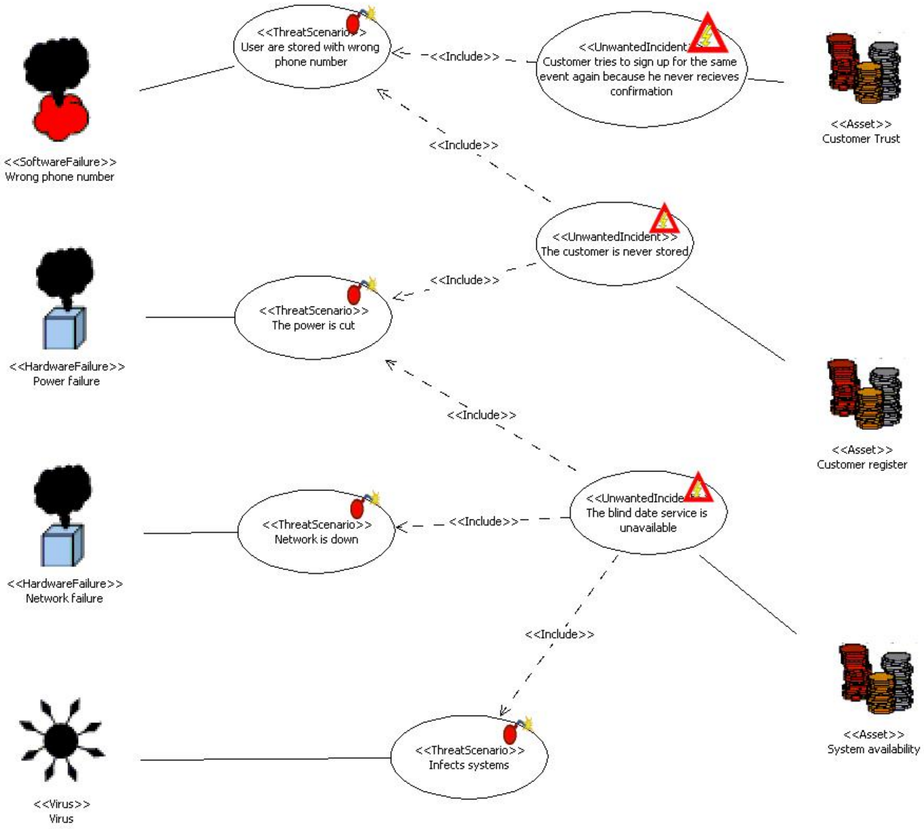
Table 6: HazOp Table

HazOp ID	Asset ID	Reference	Guideword	Threat	Incident	Scenario
R1	Customer Trust	sd RegisterCustomer, message Sms(,,)	Unintentional	Wrong phone number	Customer tries to sign up for the same event again because he never receives confirmation	User are stored with wrong phone number
R2	Customer Trust	sd JoinEvent, message Sms(..)	Delay	Wrong clock/date in the system	Customer receives notification of events that are finished	The system's clock/date is not synchronized with the customer
R3	Customer Trust	sd JoinEvent, message Sms(..)	Delay	Wrong clock/date in the system	Customer receives notification too early	The system's clock/date is not synchronized with the customer
R4	Customer Trust	sd NotifyCustomers, message GetLocation(...)	Unintentional	GetLocation returns wrong route	Incorrect route information sent to customer	Wrong position is retrieved for the customer
R5	Customer register	sd RegisterCustomers, message Sms(...)	Unintentional	Wrong phone number	The customer is never stored	User are stored with wrong phone number
R6	Customer register	sd RegisterCustomers, message Sms(...)	Loss	Power failure	The customer is never stored	The power is cut
R7	Event register	sd MakeEvent, message MakeEvent(...)	Delay	Wrong clock/date in the system	A event that is back in time is created	The system's clock/date is not synchronized with the customer
R8	Event register	sd MakeEvent, message MakeEvent(...)	Loss/Delay	Hacker	Customer is sent to the wrong place	Create event with wrong location
R9	Event register	sd MakeEvent, message MakeEvent(...)	Deliberate	Hacker	Customer is signed up for an event that does not exist	Create fake event
R10	System availability	Blind date system	Loss/Delay	Power failure	The blind date service is unavailable	The power is cut
R11	System availability	Blind date system	Loss/Delay	Network failure	The blind date service is unavailable	Network is down
R12	System availability	Blind date system	Loss/Delay	Virus	The blind date service is unavailable	Infects systems
R13	Customer Trust	sd NotifyCustomers, message Sms(...)	Deliberate	Man in the middle	A customer receives an invalid SMS	The SMS message is tampered with
R14	Customer register	sd RegisterCustomer, message Sms(,,)	Deliberate	Man in the middle	Customer is stored with wrong phone number	The phone number in SMS is tampered with
R15	Customer Trust	sd NotifyCustomers, message Sms(...)	Loss	Transmission error	A customer receives an invalid SMS	An SMS is corrupted during transfer
R16	Reputation	sd NotifyCustomers, message Sms(...)	Deliberate	Eavesdropper	Data is collected about the user	The sms is captured
R17	Customer Trust	sd JoinEvent, message Sms(..)	Deliberate	Hacker	Customer is notified about an event he has not signed up for	Sign another user on an event
R18	Physical	Blind date system	Deliberate	Thief	Equipment is stolen	Theft
R19	System availability	Blind date system	Deliberate	Thief	Equipment is stolen	Theft
R20	Physical	Blind date system	Deliberate	Thief	Data is collected about the customer	Thief finds information about the customer

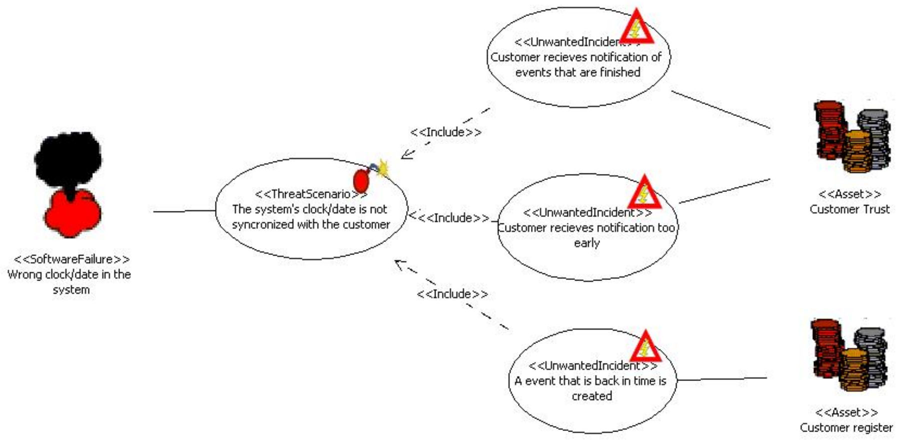
HazOp ID	Asset ID	Reference	Guideword	Threat	Incident	Scenario
R21	System availability	Blind date system	Deliberate	Thief	Data is collected about the customer	Thief finds information about the customer
R22	Reputation	Blind date system	Deliberate	Thief	Data is collected about the customer	Thief finds information about the customer
R23	Physical	Blind date system	Unintentional	Disc crash	All data erased	Hardware failure
R24	System availability	Blind date system	Unintentional	Disc crash	All data erased	Hardware failure
R25	Customer register	Blind date system	Unintentional	Disc crash	All data erased	Hardware failure
R26	Event register	Blind date system	Unintentional	Disc crash	All data erased	Hardware failure

2.2 Threat Model

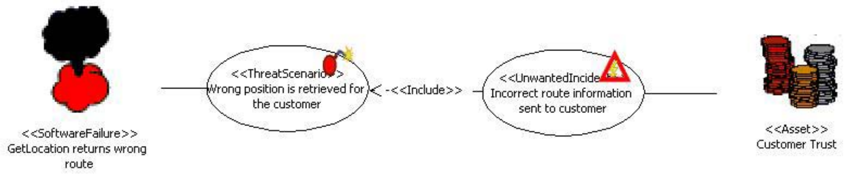
Type:	UML Model
Name:	Threat Model
Short description:	Threat model
Concern:	Threats
Full description:	This section organizes and illustrates in UML diagrams the threats that were listed in the HazOp table.



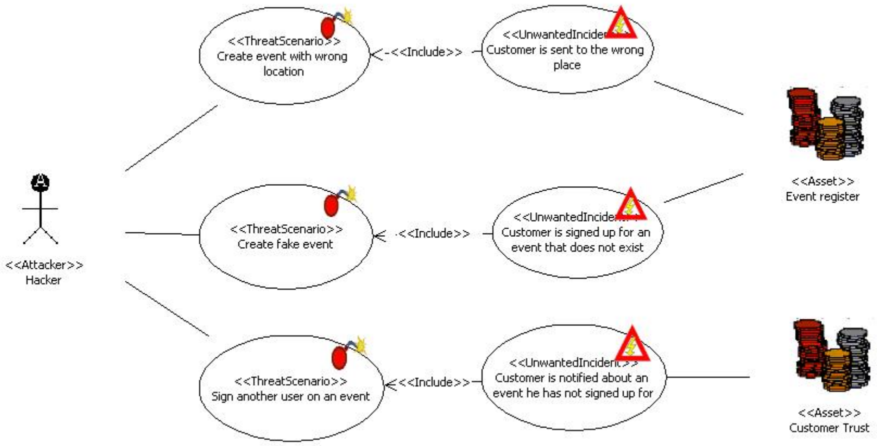
Figur 1 illustrates possible consequences relate to different kinds of hardware and software failure.


<<UnwantedIncident>>
Customer recieves notification of events that are finished
<<Include>>
<<ThreatScenario>>
The system's clock/date is not syncronized with the customer
<<Include>>
<<UnwantedIncident>>
Customer recieves notification too early
<<Asset>>
Customer Trust
<<SoftwareFailure>>
Wrong clock/date in the system
<<Include>>
<<UnwantedIncident>>
A event that is back in time is created
<<Asset>>
Customer register

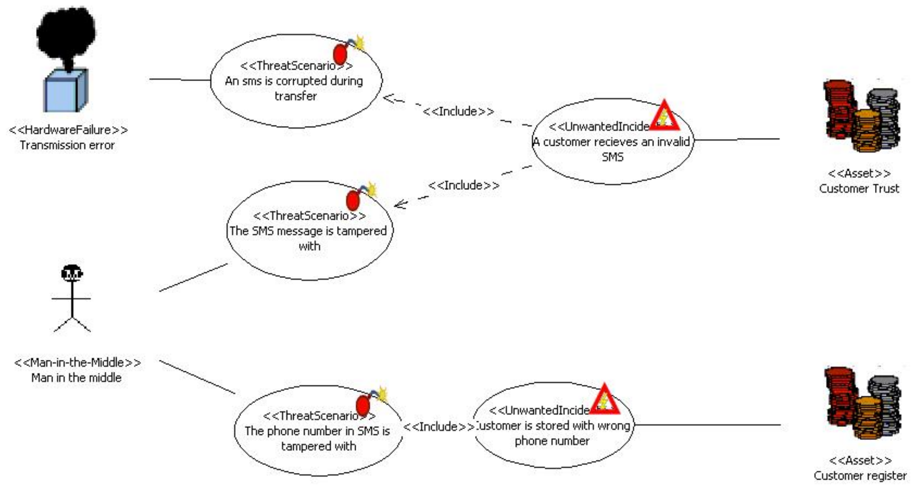
Figur 2 illustrates possible consequences of incorrect time in the system.


<<ThreatScenario>>
Wrong position is retrieved for the customer
<<Include>>
<<UnwantedIncident>>
Incorrect route information sent to customer
<<Asset>>
Customer Trust
<<SoftwareFailure>>
GetLocation returns wrong route

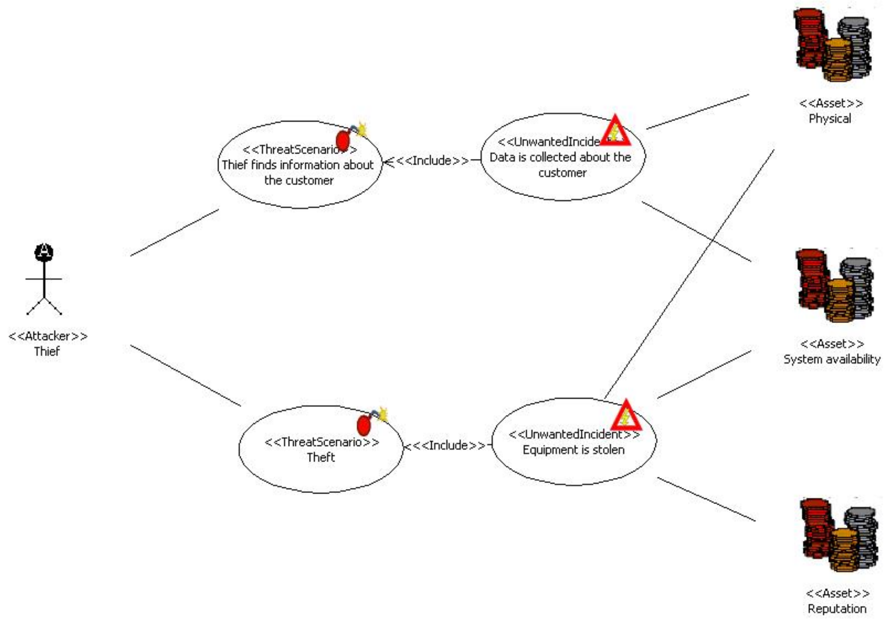
Figur 3 illustrates possible consequences of incorrect information from external system.



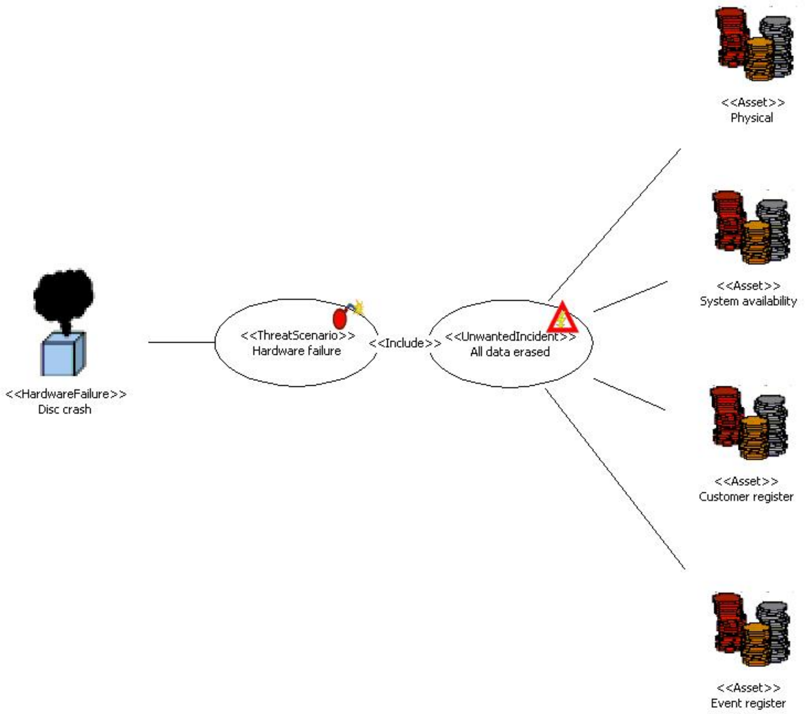
Figur 4 illustrates possible consequences of hacker attacks.



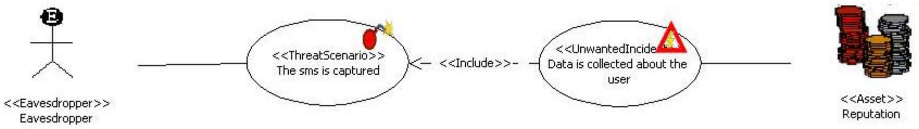
Figur 5 illustrates possible risks related to transmission and man in the middle vulnerabilities.



Figur 6 illustrates different threats a thief would have on the system



Figur 7 illustrates the impact of serious hardware failure.



Figur 8 illustrates problems with leaky transmissions.

3 Risk analysis

3.1 Consequence and Frequency Table

Type:	Table
Name:	Consequence and Frequency Table
Short description:	Consequences and Frequency table
Concern:	Consequence
Full description:	In this table we evaluate the consequences potential hazards may have for an unprotected system and the frequency with which we believe they may occur.

Table 7: Consequence and Frequency Table

Risk ID	Asset ID	Threat	Incident	Consequence Value	Frequency Value
R1	Customer Trust	Wrong phone number	Customer tries to sign up for the same event again because he never receives confirmation	Minor	Rare
R2	Customer Trust	Wrong clock/date in the system	Customer receives notification of events that are finished	Moderate	Rare
R3	Customer Trust	Wrong clock/date in the system	Customer receives notification too early	Minor	Rare
R4	Customer Trust	GetLocation returns wrong route	Incorrect route information sent to customer	Moderate	Likely
R5	Customer register	Wrong phone number	The customer is never stored	Moderate	Rare
R6	Customer register	Power failure	The customer is never stored	Moderate	Unlikely
R7	Event register	Wrong clock/date in the system	A event that is back in time is created	Moderate	Rare
R8	Event register	Hacker	Customer is sent to the wrong place	Moderate	Possible
R9	Event register	Hacker	Customer is signed up for an event that does not exist	Minor	Possible
R10	System availability	Power failure	The blind date service is unavailable	Major	Rare
R11	System availability	Network failure	The blind date service is unavailable	Major	Rare
R12	System availability	Virus	The blind date service is unavailable	Major	Possible
R13	Customer Trust	Man in the middle	A customer receives an invalid SMS	Minor	Rare
R14	Customer register	Man in the middle	Customer is stored with wrong phone number	Moderate	Rare
R15	Customer Trust	Transmission error	A customer receives an invalid SMS	Moderate	Unlikely
R16	Reputation	Eavesdropper	Data is collected about the user	Moderate	Rare
R17	Customer Trust	Hacker	Customer is notified about an event he has not signed up for	Minor	Possible
R18	Physical	Thief	Equipment is stolen	Major	Rare
R19	System availability	Thief	Equipment is stolen	Major	Rare
R20	Physical	Thief	Data is collected about the user	Moderate	Unlikely
R21	System availability	Thief	Data is collected about the user	Moderate	Unlikely
R22	Reputation	Thief	Data is collected about the user	Moderate	Unlikely
R23	Physical	Disc crash	All data erased	Catastrofic	Unlikely
R24	System availability	Disc crash	All data erased	Catastrofic	Unlikely
R25	Customer register	Disc crash	All data erased	Catastrofic	Unlikely
R26	Event register	Disc crash	All data erased	Catastrofic	Unlikely

4 Risk evaluation

4.1 Risk estimate

Type:	Table
Name:	Risk estimate
Short description:	Risk estimate
Concern:	Risk estimates
Full description:	Based on the risk matrix and the consequence and frequency table, we can calculate an estimated risk value, which tells us how critical a risk is.

Table 8: Risk Evaluation Table

Risk ID	Risk Value
R1	Low
R2	Low
R3	Low
R4	Moderate
R5	Low
R6	Low
R7	Low
R8	Moderate
R9	Low
R10	Major
R11	Major
R12	Major
R13	Low
R14	Low
R15	Low
R16	Low
R17	Low
R18	Major
R19	Major
R20	Moderate
R21	Moderate
R22	Moderate
R23	Major
R24	Major
R25	Major
R26	Major

5 Risk treatment

5.1 Risk Treatment Table

Type: Table
Name: Risk Treatment Table
Short description: Risk treatment
Concern: Treatment
Full description: Using the risk evaluation table and the risk evaluation table, we have identified the 9 most critical threats to the system. In this table we propose ways to address these threats and reduce the value of the risks.

Formatert: Skrift: 10 pt

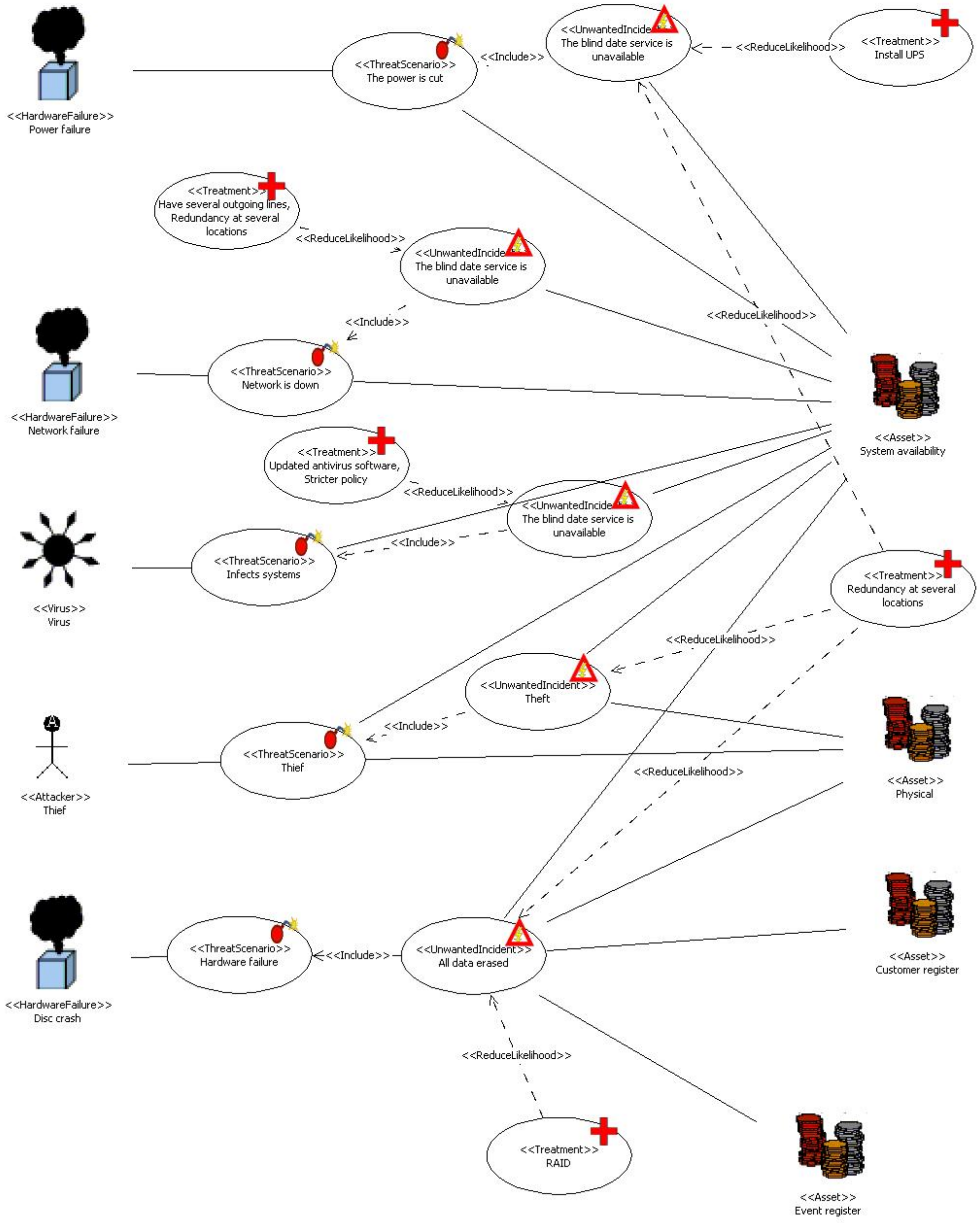
Table 9: Treatment Identification Table

Treatment ID	Risk ID/category	Treatment strategy	Description
T1	R10	Reduce frequency	Install UPS, Redundancy at several locations
T2	R11	Reduce frequency	Have several outgoing lines, Redundancy at several locations
T3	R12	Reduce frequency	Updated antivirus software, Stricter policy
T4	R18	Reduce consequence	Redundancy at several locations
T5	R19	Reduce consequence	Redundancy at several locations
T6	R23	Reduce consequence	RAID, Redundancy at several locations
T7	R24	Reduce consequence	RAID, Redundancy at several locations
T8	R25	Reduce consequence	RAID, Redundancy at several locations
T9	R26	Reduce consequence	RAID, Redundancy at several locations

Install UPS: Install an external power supply which can provide power in case of power loss.
Redundancy at several locations: Having several servers at different locations eliminates the single point of failure and increases the uptime.
Updated antivirus software: Making sure that the antivirus software is updated at a regular basis.
Stricter policy: Strict user policy will prevent users from installing/running unnecessary programs and therefore reduce the likelihood of virus, Trojans, worms, programs exploits etc.
RAID (*Redundant Array of Inexpensive (Independent) Disks):* Several independent disks storing the same data will reduce the frequency of a critical disc crash.

5.2 Treatment Model

Type:	UML Model
Name:	Treatment Model
Short description:	Treatment model
Concern:	Treatment
Full description:	Treatments described in Risk treatment table shown as UML diagram.



Figur 9 shows how the proposed treatments address threats.