Instituto Tecnológico de Aeronáutica

Extending STPA with STRIDE to Identify Cybersecurity Loss Scenarios of an Electronic Voting System by Smartphone (SiVES)

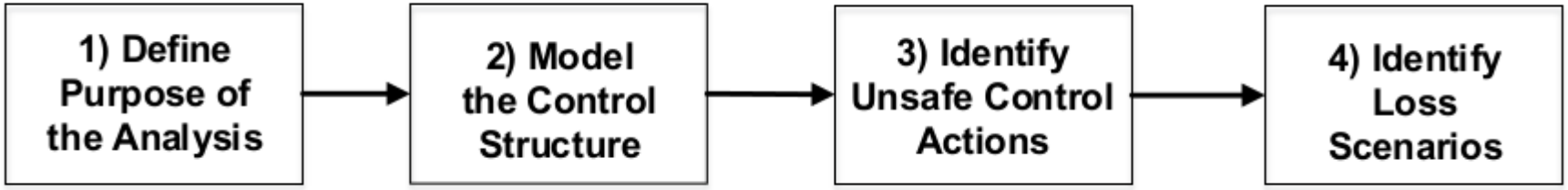
Master Student: Nivio Paula de Souza
Advisor: PhD Celso Massaki Hirata
Co-advisor: PhD Cecília de Azevedo Castro César

Overview

The objective of this work is to specialize STPA by extending it with already established models (STRIDE) to investigate, find and define relevant cybersecurity requirements.

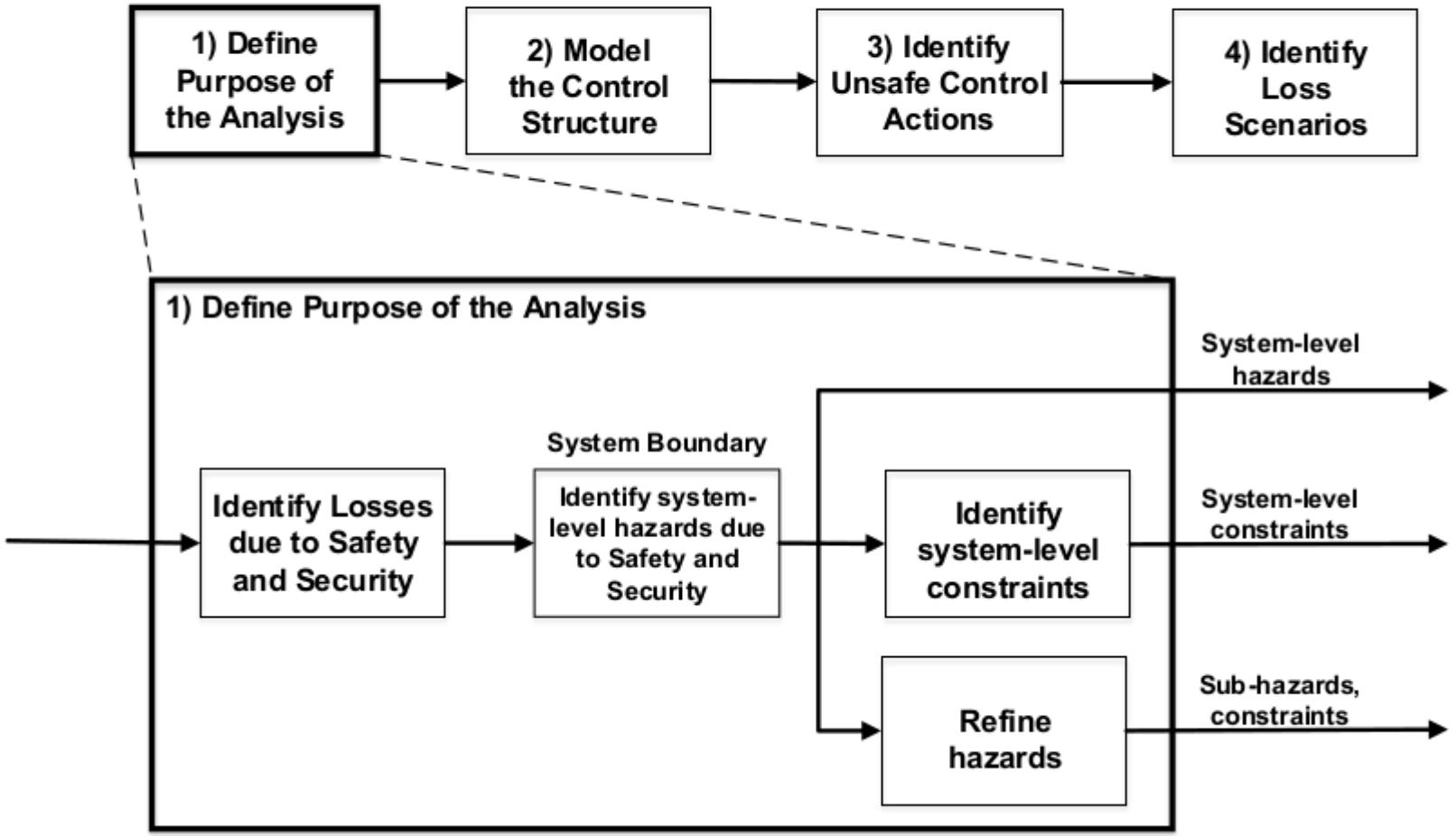
Depicting the process

Generic STPA Steps



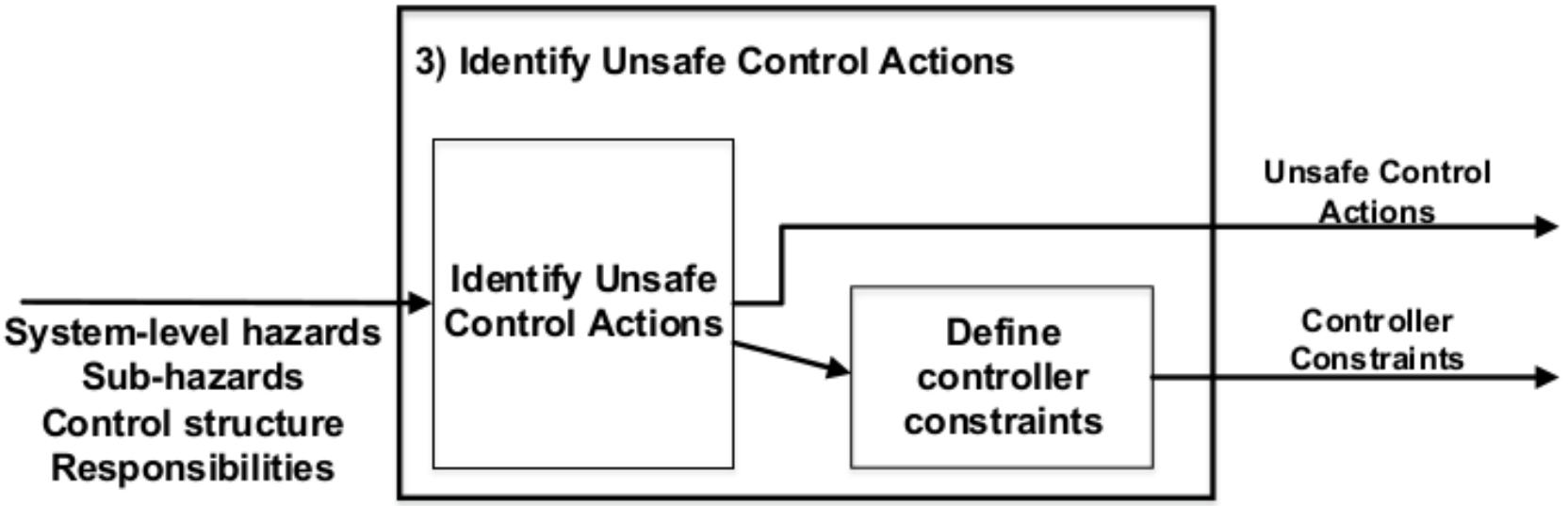
Depicting the process

Define Purpose of the Analysis – In Detail



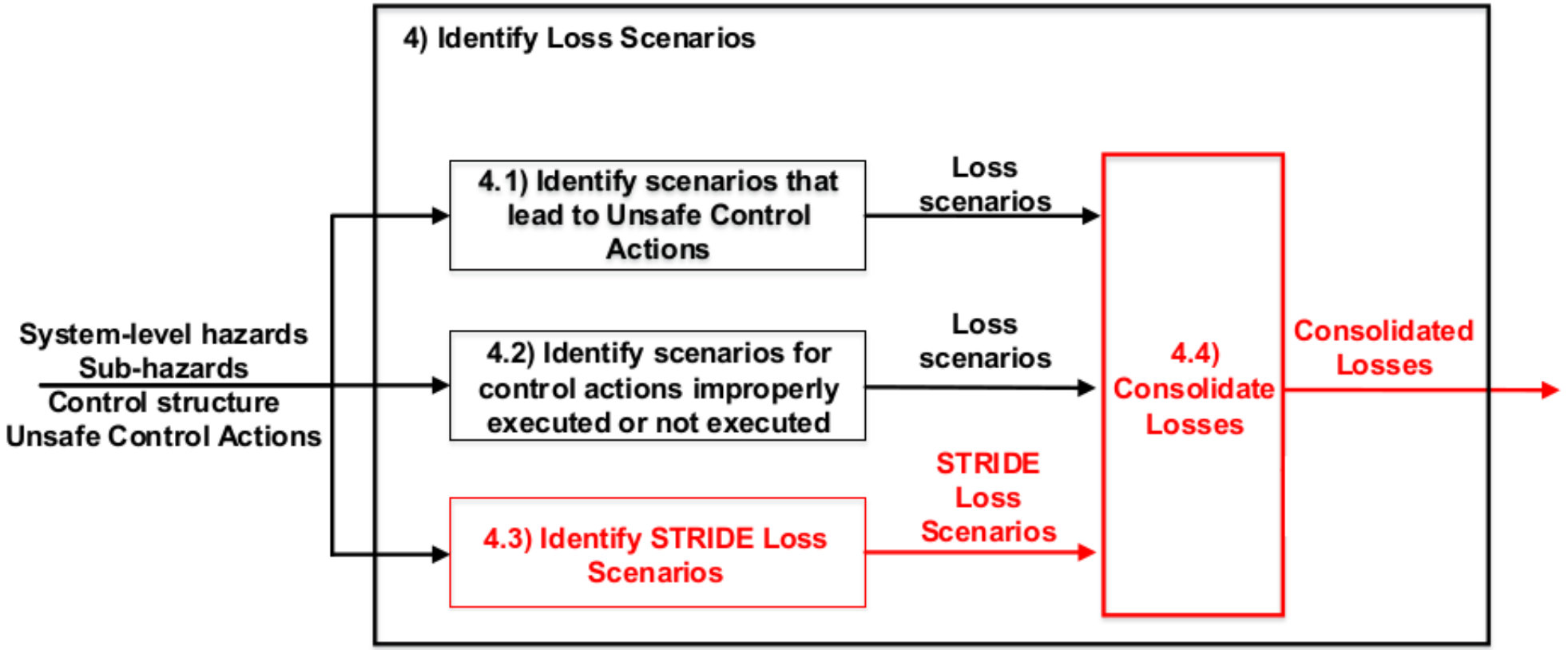
Depicting the process

Identify Unsafe Control Actions – In Detail

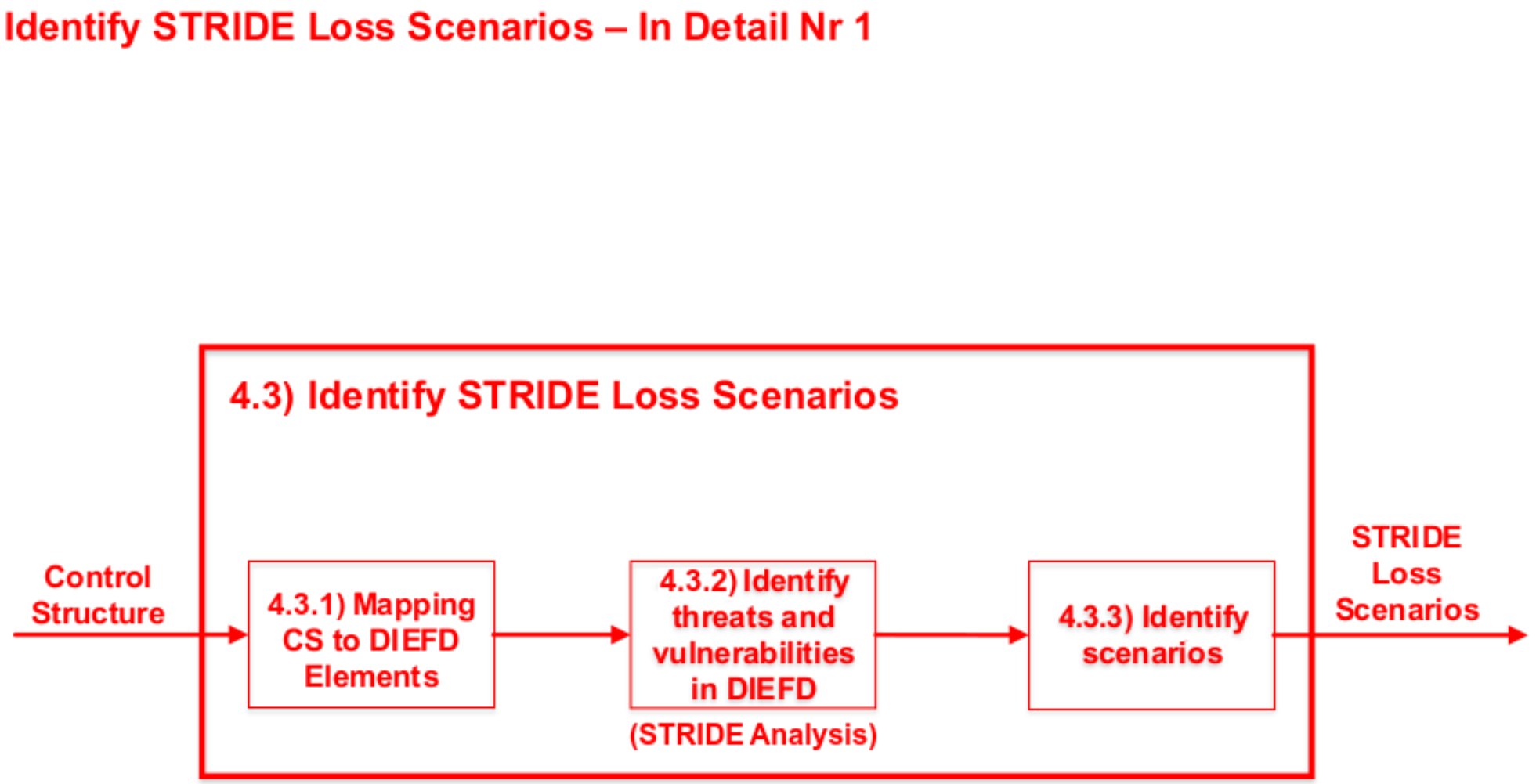


Depicting the process

Identify Loss Scenarios – Overview



Depicting the process



Explaining the process

Before explaining the process, we need to present how analysis is organized:

1th Level – Steps

2nd Level – Activities

3rd Level – Tasks

4th Level – Subtasks

Explaining the process

For simplicity, in this presentation, we will use the STEP nomenclature for each first level part of STPA, as presented in the STPA Handbook.

Initially, execute 3 steps: “Define Purpose of the Analysis”, “Model the Control Structure” and “Identify Hazardous Control Actions”.

We will perform the Step “Identify Loss Scenarios”.

Inside this Step Nr 4, there are 3 activities:

4.1) Identify scenarios that lead to Hazardous Control Actions

4.2) Identify scenarios for control actions improperly executed or not executed

4.3) Identify STRIDE Loss Scenarios

Explaining the process

The activity Nr 4.3, Identify STRIDE Loss Scenarios there 3 tasks in sequence:

Task 4.3.1: The model elements were raised in “Model the Control Structure” and they will now be mapped to Process, External Entity, Data Flow and Data Store for DIEFD generation.

Task 4.3.2: Identify threats and vulnerabilities in DIEFD (STRIDE Analysis)

Task 4.3.3: Identify scenarios

In Task Nr 4.3.3, the interactions already analyzed in STRIDE will be analyzed one by one (from the perspective of 4 tuples) for each pair of elements, so that all flows are covered and then each element will be analyzed individually in this way to causal factors associated.

Explaining the process

In final activity 4.4) Consolidate Losses, the results of the previous activities, tasks and subtasks will be related to the HCA and the 3-tuple in order to evaluate (Right and Group 2 (Left Side) → Control Circuit and Information Lifecycle) and reveal the security scenarios. Also in this activity, there will be a redundancy check with the scenarios generated by all activities Nr 4.X (STPA + STRIDE), to verify if the scenario is new (NEW), or if it is repeated (with STPA or with STRIDE itself) (REP) and should be discarded. Finally, only scenarios classified as NEW will be used.

Explaining the process

NOTE: From here, for the visualization does not get polluted and according to the convenience, we can use the following abbreviations:

Process → Proc

External Entity → EE

Data Store → DS

Data Flow → DF

Process to identify the security requirements - Overview

The process to identify the security requirements is:

- Execute steps 1, 2 and 3
- Execute activities 4.1 and 4.2 from STPA Step 4
- Map model elements and obtain the DFD (DIEFD) from CS (Task 4.3.1)
- Identify threats and vulnerabilities in DIEFD (STRIDE Analysis) (Task 4.3.2)
- Identify scenarios (Task 4.3.3)
- Consolidate Losses (Activity 4.4): for each HCA, verify which 3-tuple can be a causal factor. If it can be, generate a requirement (recommendation) with redundancy check (NEW and REP states)

Process to identify the security requirements - Overview

The process to identify the security requirements is:

- Execute steps 1, 2 and 3
- Execute activities 4.1 and 4.2 from STPA Step 4
- Map model elements and obtain the DFD (DIEFD) from CS (Task 4.3.1)
- Identify threats and vulnerabilities in DIEFD (STRIDE Analysis) (Task 4.3.2)
- Identify scenarios (Task 4.3.3)
- Consolidate Losses (Activity 4.4): for each HCA, verify which 3-tuple can be a causal factor. If it can be, generate a requirement (recommendation) with redundancy check (NEW and REP states)

Important Outputs from 3 first steps

1) Control Actions
2) Hazardous Control Actions (HCA)
3) Model Elements
4) Control Structure (CS)

Initial Analysis Step (Define Purpose of Analysis)

System purpose and goal

System to allow voting of users using smartphones, meeting electoral justice requirements, through the installation, authentication, operation (voting), and verification methods to contribute to the Brazilian democracy.

"A system to do {What = Purpose} by means of {How = Method} in order to contribute to {Why = Goals}"

We will restrict to the presidential election.

The modelling can be applied to any device, but we use smartphone.

Initial Analysis Step (Define Purpose of Analysis)

Define and frame the problem

Scenario: Assure that electronic voting by smartphone meets the legal requirements of security through its attributes (confidentiality[1] and integrity[2] and availability) in the voting process.

Mission: Carry out electronic voting, meeting the requirements of the law and security, allowing a more convenient alternative for citizens to express their citizenship through voting.

Key stakeholders: Voters, TSE, STI and virtual stores (Apple Store and Google Play).

System purpose and goals: System to allow voting of users using smartphones, meeting electoral justice requirements, through the installation, authentication, operation (voting), and verification methods to contribute to the Brazilian democracy.

1 - Resolution Nr 20.997/02, instruction Nr 61 – TSE (http://www.tse.jus.br/legislacao-tse/res/2002/RES209972002.htm)
2 – Provided by Law Nr 13.165/2015 (printed vote)

Initial Analysis Step (Define Purpose of Analysis)

Define and frame the problem

The Brazilian Law does not define concepts such as privacy and anonymity. In juridical matters, the definition of each concept is the responsibility of the judge in the case, allowing each judge to interpret it, as long as there is no jurisprudence of higher courts.[1]

(1) DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006. p. 109-113

Initial Analysis Step (Define Purpose of Analysis)

DEFINITIONS USED IN THIS ANALYSIS:

Security is known by its attributes (availability, integrity and confidentiality):

Availability[1]: readiness for correct service

Integrity[1]: absence of improper system alterations

Confidentiality[1]: absence of unauthorized disclosure of information

Verifiability of the electronic voting system: method that allows the voter to verify his/her vote inside Electoral Office, after counting, providing security and anonymity.

(1) Avizienis at all. Basic Concepts and Taxonomy of Dependable and Secure Computing. IEEE Transactions on Depandaple and Secure Computing, Vol. 1, NO. 1. January-March 2004.

Initial Analysis Step (Define Purpose of Analysis)

DEFINITIONS USED IN THIS ANALYSIS:

STRIDE[1]

“The STRIDE method is proposed by Microsoft and represents a mnemonic for six different types of security threats: Spoofing: Masquerading of a legitimate user, process or system element, Tampering: Modification/editing of legitimate information, Repudiation: Denying or disowning a certain action executed in the system, Information disclosure: Data breach or unauthorized access to confidential information, Denial of Service (DoS): Disruption of service for legitimate users, and Elevation of privilege: Getting higher privilege access to a system element by a user with restricted authority. STRIDE analyzes vulnerabilities against each system component which could be exploited by an attacker to compromise the whole system.”

(1) Khan et all. STRIDE-based Threat Modeling for Cyber-Physical Systems. Queen University Belfast.

Initial Analysis Step (Define Purpose of Analysis)

DEFINITIONS USED IN THIS ANALYSIS:

Security threats always have already been defined previously (STRIDE)[1]:

Spoofing: An example of identity spoofing is illegally accessing and then using another user's authentication information, such as username and password.

Tampering: Data tampering involves the malicious modification of data. Examples include unauthorized changes made to persistent data, such as that held in a database, and the alteration of data as it flows between two computers over an open network, such as the Internet.

Repudiation: Repudiation threats are associated with users who deny performing an action without other parties having any way to prove otherwise—for example, a user performs an illegal operation in a system that lacks the ability to trace the prohibited operations. Nonrepudiation refers to the ability of a system to counter repudiation threats. **For example, a user who purchases an item might have to sign for the item upon receipt**. The vendor can then use the signed receipt as evidence that the user did receive the package.

Information disclosure: Information disclosure threats involve the exposure of information to individuals who are not supposed to have access to it—for example, the ability of users to read a file that they were not granted access to, or the ability of an intruder to read data in transit between two computers.

Denial of service: Denial of service (DoS) attacks deny service to valid users—for example, by making a Web server temporarily unavailable or unusable. You must protect against certain types of DoS threats simply to improve system availability and reliability.

Elevation of privilege: In this type of threat, an unprivileged user gains privileged access and thereby has sufficient access to compromise or destroy the entire system. Elevation of privilege threats include those situations in which an attacker has effectively penetrated all system defenses and become part of the trusted system itself, a dangerous situation indeed.

(1) MICROSOFT, The STRIDE Threat Model, December 2009. Available https://docs.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20). Accessed September, 2018.

Initial Analysis Step (Define Purpose of Analysis)

Basic system description

The description includes the identification of system's elements, their responsibilities, and control relationships.

Initial Analysis Step (Define Purpose of Analysis)

Basic system description

SiVES is a smartphone electronic voting system based on the following assumptions:

1. The current Brazilian Electronic Voting System security is considered to be acceptable. We do not consider it in our analysis;

2. The process of biometric registration of voters is not considered in the analysis. We consider that eligible users of SiVES have their biometric data registered.

3. SiVES consists of 4 methods: preparation; operation (authentication and voting); tallying; and verification.

4. SiVES must allow the voter to verify that the system has counted his/her vote correctly (verifiability) keeping confidentiality, integrity and availability (primary attributes) and anonymity and privacy (secondary attributes).

Initial Analysis Step (Define Purpose of Analysis)

Basic system description

5. SiVES has the server component (SiVES-S) that runs on server computers in STI in Brasília and the client component (SiVES-C) that runs on the voter's smartphone. SiVES denotes the system, including the server and client components.

6. The voting process allows "revotation" to mitigate voting under duress. The valid vote is the last vote submitted by SiVES.

7. The possible voting options are: blank, null, or a valid candidate.

8. SiVES is available to voters for a given period. Afterwards, only the presential voting is possible, which must be made in a specific day.

9. On the day of the presential voting, SiVES is no longer available.

10. The verification of vote occurs in verification machines inside electoral offices and after the end of voting process.

11. This description follows partly the Estonian model of electronic voting[1, 2 e 3].

12. Some limitations are accepted to facilitate this analysis, as long as they do not affect availability, confidentiality, and integrity.

(1) https://www.nexojornal.com.br/expresso/2017/02/19/Como-a-Estônia-se-transformou-num-laboratório-de-eleições-on-line
(2) https://e-estonia.com/solutions/e-governance/i-voting/
(3) https://time.com/5541876/estonia-elections-electronic-voting/

Analysis – Model the Control Structure

CS Description Methods

The development is not addressed. We assume that SiVES is already developed. In the Preparation Method, we assume the following phases:

- Registration of biometric data's voters in the electoral office
- System set up
- Call for votation
- App instalation

For brevity of analysis, we are not going to consider the phase of registration of biometric data's voters in the electoral office for elaborating the Control Structure. We assume that voter fingerprint has already been captured and voter biometric data are already available.

Analysis – Model the Control Structure

CS Description Methods

Preparation: System set up is about installing all the hardware and software, including the network, to run the server system. It also includes the upload in the app stores. Call for voting is the public call to all the voters. It is the responsibility of TSE. Application installation refers to installation of the app in the smartphone. Smartphone user makes it.

Operation: voter authenticates in the system and votes.

Tallying: STI tallies the votes and TSE makes the results public. (it will be considered for the CS, but it will not be analysed)

Verification: voter, if he/she wishes, goes to the electoral office and checks his/her vote.

Define Purpose of the Analysis

For Steps 1, 2 and 3 we will perform the analysis of Preparation, Voting and Verification methods **are methods where the voters interact with the system**.

1) Unacceptable Losses Identification

a) Identify Unacceptable Losses that violate Safety

b) Identify Unacceptable Losses that violate Security attributes or according to STPA analysis

c) Identify Unacceptable Losses that violate Security attributes or according to Security Threats using STRIDE

d) Identify Unacceptable Losses that violate Privacy attributes

Define Purpose of the Analysis

2) Hazards Identification

a) Identify hazards related to Safety, Security, and Privacy

3) Application of Step 3 to identify Hazardous Control Actions

4) Application of Step 4 to identify scenarios, identify associated causal factors and generate recomendations

Define Purpose of the Analysis

Unacceptable Security and Privacy Losses

UL1: Unacceptable number of eligible voters who are unable to vote (denial of service → availability and reliability).

UL2: Unacceptable number of eligible voters who are unable to verify the vote (denial of service → availability and reliability).

UL3: Loss of credibility due to unacceptable number and severity of security issues (spoofing, information disclosure and tampering → authentication, confidentiality and integrity).

UL4: Loss of credibility due to violation of privacy (linkability – by inference → unlinkability and non-repudiation – irrefutable evidence concerning voter's vote → plausible deniability)

Define Purpose of the Analysis

Hazards

H1: Voters unable to vote (reliability, availability and mission assurance issues)

H1.1: State that does not allow a legitimate voter to vote (to assure the mission)

H1.2: State that prevents the vote due to the system's unavailability and reliability issues (denial of service → availability and reliability)

H2: Voters unable to verify the vote (reliability, availability and mission assurance issues)

H2.1: State that does not allow a legitimate voter who voted to verify his/her own vote (to assure the mission)

H2.2: State that prevents to verify the vote due to the system's unavailability and reliability issues (denial of service → availability and reliability)

Define Purpose of the Analysis

Hazards

H3: State that allows security violations (security issues)

H3.1: State that allows unauthorized access to private information (data, vote, etc.) (information disclosure → confidentiality)

H3.2: State that allows an unauthorized person to vote (spoofing → authentication and authorization)

H3.3: State that allows for undue alteration of the voter's vote (tampering → integrity)

H4: State that allows data privacy loss (privacy issues)

H4.1: State that allows information disclosure that links voter to vote (linkability → unlinkability)

H4.2: State that does not allow a voter to deny to whom he/she voted for (non-repudiation → plausible deniability)

Define Purpose of the Analysis – Mapping Unacceptable Losses to Hazards to Constraints

Goal	Losses	Hazards	Constraints
System to allow voting of users using smartphones, meeting electoral justice requirements, through the System Set Up, Call for Votation and app installation, Operation and Verifiability methods to contribute to the Brazilian democracy.	UL1: Unacceptable number of eligible voters who are unable to vote	H1: Voters unable to vote (reliability, availability and mission assurance issues)	C1: System must allow a voter to vote
		H1.1: State that does not allow a legitimate voter to vote (to assure the mission)	C1: System must allow a voter to vote
		H1.2: State that prevents the vote due to the system's unavailability and reliability issues (denial of service → availability and reliability)	C2: System must remain available for the voter to vote
	UL2: Unacceptable number of eligible voters who are unable to verify the vote	H2: Voters unable to verify the vote (reliability, availability and mission assurance issues)	C3: System must allow voter verifies the vote
		H2.1: State that does not allow a legitimate voter who voted to verify his/her own vote (to assure the mission)	C3: System must allow voter verifies the vote
		H2.2: State that prevents to verify the vote due to the system's unavailability and reliability issues (denial of service → availability and reliability)	C4: System must remain available for the voter to verify the own vote

Define Purpose of the Analysis – Mapping Unacceptable Losses to Hazards to Constraints

Goal	Losses	Hazards	Constraints
System to allow voting of users using smartphones, meeting electoral justice requirements, through the System Set Up, Call for Votation and app installation, Operation and Verifiability methods to contribute to the Brazilian democracy.	UL3: Loss of credibility due to unacceptable number and severity of security issues	H3: State that allows security violations (security issues)	C5: System must prevent security violations
		H3.1: State that allows unauthorized access to private information (data, vote, etc.) (information disclosure → confidentiality)	C6: System must prevent unauthorized access to private information
		H3.2: State that allows an unauthorized person to vote (spoofing → authentication and authorization)	C7: System must prevent an unauthorized person to vote
		H3.3: State that allows for undue alteration of the voter's vote (tampering → integrity)	C8: System must prevent undue alteration of the voter's vote

Define Purpose of the Analysis – Mapping Unacceptable Losses to Hazards to Constraints

Goal	Losses	Hazards	Constraints
System to allow voting of users using smartphones, meeting electoral justice requirements, through the System Set Up, Call for Votation and app installation, Operation and Verifiability methods to contribute to the Brazilian democracy.	UL4: Loss of credibility due to violation of privacy (linkability – by inference → unlinkability and non-repudiation – irrefutable evidence concerning voter's vote → plausible deniability)	H4: State that allows data privacy loss (privacy issues)	C9: System must prevent data privacy loss
		H4.1: State that allows information disclosure that links voter to vote (linkability → unlinkability)	C10: System must prevent information disclosure that leads to identify voters' vote
		H4.2: State that does not allow a voter to deny to whom he/she voted for (non-repudiation → plausible deniability)	C11: System must prevent information disclosure that links voters to their votes

Analysis (Model the CS) **(Identify Model Elements)**

→ **"A system to do {What = Purpose} by means of {How = Method} in order to contribute to {Why = Goals}"**

→ An electronic system that allows voters to vote from their smartphone, maintaining confidentiality, integrity, anonymity, and availability by means of installing the application, voter authentication and operation (voting), in order to contribute to the process electoral.

Method	Model Elements	Description
System set up, call for votation and app installation	TSE, STI, Virtual Stores, Voter, *Smartphone* (*)	Elements that have responsibilities in the system set up, call for votation and app installation
Voting	STI, SiVES-S, SiVES Servers (**), SiVES-C, Voter	Elements that have responsibilities in the voting
Tallying	TSE, STI, SiVES-S	Elements that have responsibilities in the tallying
Verification	STI, Electoral Zone, Verification Machine, Verification Machine Software (VMS) (***), SiVES-S, SiVES Servers (**), Voter	Elements that have responsibilities in the verification

(*) Whenever the term smartphone is quoted, it refers to the set plus hardware operating system (Android or IOS). For analysis to be treatable, it has been admitted that the operating system is up to date and use the required security measures (anti-malware, firewall, etc.). **That is, it was considered the smartphone secure**.

(**) We assume that the operating system servers and hardware that support SiVES are secure, are up to date and use the required security measures (anti-malware, firewall, etc.).

(***) We assume that the Verification Machine operating system and hardware that support VMS are secure, are up to date and use the required security measures (anti-malware, firewall, etc.).

Analysis (Model the CS) **(Identify responsibilities)**

Model Element	**Responsibility for "Preparation"**
TSE	- Validate SiVES - Request changes to STI - Call for participation in mobile election
STI (*)	- Update SiVES when requested by TSE - Generate SiVES-C installation package - Send SiVES-C installation package to Virtual Stores
Virtual Stores	- Make SiVES-C available
Voter	- Follow security and privacy TSE guidelines - Request SiVES-C installation package to smartphone - Request updates when available
Smartphone (**)	- Request SiVES-C installation package file - Present installation status message

(*) Uploading the installation packages to the virtual stores was considered in CS, but it will not be part of the scope of this analysis.

(**) We assume that the smartphone is always operational. It is not part of our analysis.

Analysis (Model the CS) **(Identify responsibilities)**

Model Element	**Responsibility for "Operation (Voting)"**
STI	- Make SiVES-S available to voting method
Voter (*)	- Follow security and privacy TSE guidelines - Authenticate - Accept the privacy agreement - Vote
SiVES-C	- Capture biometric data for SiVES-C - Send request of authentication to SiVES-S - Present result of the authentication - Offer privacy agreement - Send the acceptance of the privacy agreement to SiVES-S - Send the vote - Present voting confirmation or error
SiVES-S	- Provide authentication - Send result of the authentication - Register the acceptance of the privacy agreement - Register the vote sent by SiVES-C - Send the voting confirmation or error

All of the above responsibilities should ensure ***security*** and ***privacy*** based on their attributes (availability, confidentiality, integrity, unlinkability, anonymity, pseudonymity, plausible deniability, undetectability, unobservability, confidentiality, content awareness, consent compliance property)

Analysis (Model the CS) **(Identify responsibilities)**

Model Element	**Responsibility for "Tallying"**
TSE	- Present voting results to voters
STI	- Make SiVES-S available to tallying method - Request Tallying - Inform of the availability of the voting results to TSE
SiVES-S	- Tally the votes - Make the results available (The types of results (reports) are specified by TSE)

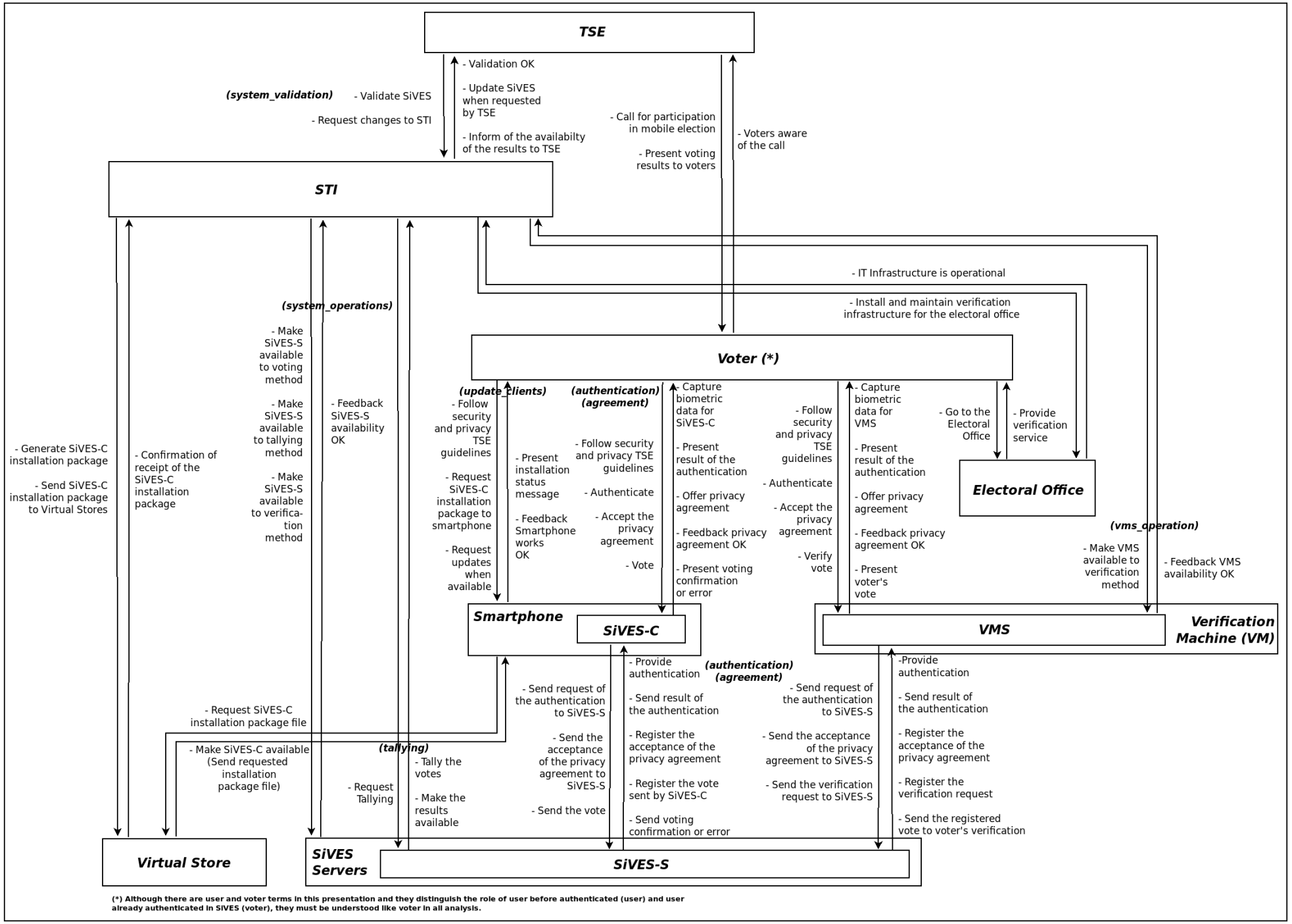
All of the above responsibilities should ensure ***security*** and ***privacy*** based on their attributes (availability, confidentiality, integrity, unlinkability, anonymity, pseudonymity, plausible deniability, undetectability, unobservability, confidentiality, content awareness, consent compliance property)

Analysis (Model the CS) **(Identify responsibilities)**

Model Element	Responsibility for “Verification”
STI	- Make SiVES-S available to verification method - Make VMS available to verification method - Install and maintain verification infrastructure for the electoral office
SiVES-S	- Provide authentication - Send result of the authentication - Register the privacy agreement - Register the verification request - Send the registered vote to voter's verification
Electoral Office	- Provide verification service
Voter	- Follow security and privacy TSE guidelines - Authenticate - Accept the privacy agreement - Verify vote
Verification Machine Software (VMS)	- Capture biometric data for VMS - Send request of the authentication to SiVES-S - Present result of the authentication - Offer privacy agreement - Send the acceptance of the privacy agreement to SiVES-S - Send the verification request to SiVES-S - Present voter’s vote

All of the above responsibilities should ensure ***security*** and ***privacy*** based on their attributes (availability, confidentiality, integrity, unlinkability, anonymity, pseudonymity, plausible deniability, undetectability, unobservability, confidentiality, content awareness, consent compliance property)

Analysis (Model the CS) **(Identify control relationships)**



Analysis (Model the CS) **(Identify control actions for each element)**

Method 1: Preparation

Validate SiVES; Request changes to STI; and Call for participation in mobile election		
Model Element	**Control Actions**	**CA Nr**
TSE	- Validate SiVES - Call for participation in mobile election - Provide security and privacy guidelines to voter - Request changes of SiVES to STI	01 02 03 04

Update SiVES when requested by TSE; Generate SiVES-C installation package; and Send SiVES-C installation package to Virtual Stores		
Model Element	**Control Actions**	**CA Nr**
STI	- Send SiVES-C installation package file to Virtual Stores	05

Make SiVES-C available		
Model Element	**Control Actions**	**CA Nr**
Virtual Stores	- No control action	-

Analysis (Model the CS) **(Identify control actions for each element)**

Method 1: Preparation

Request SiVES-C installation package to smartphone; Request updates when available; and Follow security and privacy TSE guidelines		
Model Element	**Control Actions**	**CA Nr**
Voter	- Follow security and privacy TSE guidelines - Install/update SiVES-C through the virtual store application when version is available (Apple Store / Google Play)	06 07 -

Request SiVES-C installation package file; and Present installation status message		
Model Element	**Control Actions**	**CA Nr**
Smartphone	- Install SiVES-C from Virtual Store	08

Analysis (Model the CS) **(Identify control actions for each element)**

Method 2: Operation (Voting)

Make SiVES-S available to voting method		
Model Element	**Control Actions**	**CA Nr**
STI	- Make and keep SiVES-S available	09

Follow security and privacy TSE guidelines; Authenticate; Accept the privacy agreement; and Vote		
Model Element	**Control Actions**	**CA Nr**
Voter	- Follow security and privacy guidelines (**repeated – CA Nr 08**) - Provide biometric data - Accept the privacy agreement - Vote - Receive voting confirmation - Finalize session	- 10 11 12 13 14

Analysis (Model the CS) **(Identify control actions for each element)**

Method 2: Operation (Voting)

Capture biometric data for SiVES-C; Send request of authentication to SiVES-S; Present result of the authentication; Offer privacy agreement; Send the acceptance of the privacy agreement to SiVES-S; Send the vote; and Present voting confirmation or error		
Model Element	**Control Actions**	**CA Nr**
SiVES-C	- Capture biometric data for authentication - Send the user's biometric data to SiVES-S - Display the SiVES-S response about user authentication - Offer the privacy agreement to the voter - Send the required acceptance of the privacy agreement to SiVES-S - Send the voter's vote to SiVES-S - Display and store voting confirmation or display error status	15 16 17 18 19 20 21

Provide authentication; Send result of the authentication; Register the acceptance of the privacy agreement; Register the vote sent by SiVES-C; and Send the voting confirmation or error		
Model Element	**Control Actions**	**CA Nr**
SiVES-S	- Validate the biometric data received with the voter database - Register the acceptance of the privacy agreement - Receive and store the vote from SiVES-C - Overwrite older vote in case of “revotation” - Finalize session in timeout case	22 23 24 25 26

Tallying method (method 3) won’t be analyzed, as mentioned previously.

Analysis (Model the CS) **(Identify control actions for each element)**

Method 4: Verification

Make SiVES-S available to verification method; Make VMS available to verification method; and Install and maintain verification infrastructure for the electoral office		
Model Element	**Control Actions**	**CA Nr**
STI	- Make and keep SiVES-S available (**repeated – CA Nr 12**) - Make and keep VMS available to verification method - Install and maintain verification infrastructure for the electoral office	- 27 28

Provide authentication; Send result of the authentication; Register the privacy agreement; Register the verification request; and Send the registered vote to voter´s verification		
Model Element	**Control Actions**	**CA Nr**
SiVES-S	- Receive biometric user data (**repeated – CA Nr 26**) - Validate the biometric data received with the voter database (**repeated – CA Nr 27**) - Respond, informing if the user is authenticated as a voter (**repeated – CA Nr 28**) - Register the acceptance of the privacy agreement (**repeated – CA Nr 29**) - Register the verification request - Finalize session in timeout case (**repeated – CA Nr 32**)	- - - - 29 -

Provide verification service		
Model Element	**Control Actions**	**CA Nr**
Electoral Office	- Provide voter’s security and privacy - Provide verification service	30 31

Analysis (Model the CS) **(Identify control actions for each element)**

Method 4: Verification

Follow security and privacy TSE guidelines; Authenticate; Accept the privacy agreement; and Verify vote		
Model Element	**Control Actions**	**CA Nr**
Voter	- Follow security and privacy guidelines (**repeated – CA Nr 08**) - Provide biometric data (**repeated – CA Nr 13**) - Accept the privacy agreement (**repeated – CA Nr 14**) - Verify the vote - Finalize session (**repeated – CA Nr 17**)	- - - 32 -

Capture biometric data for VMS; Send request of authentication to SiVES-S; Present result of the authentication; Offer privacy agreement; Send the acceptance of the privacy agreement to SiVES-S; Send the verification request to SiVES-S; and Present voter's vote		
Model Element	**Control Actions**	**CA Nr**
Verification Machine Software (VMS)	- Capture biometric data for authentication (**repeated – CA Nr 18**) - Send the user's biometric data to SiVES-S (**repeated – CA Nr 19**) - Display the SiVES-S response about user authentication (**repeated – CA Nr 20**) - Offer the privacy agreement to the voter (**repeated – CA Nr 21**) - Send the required acceptance of the privacy agreement to SiVES-S (**repeated – CA Nr 22**) - Request vote to SiVES-S	- - - - - 33

Analysis (Model the CS)

Modeling the Control Structure for Security (CS)

5) Develop Description of the Process Model
   a) Identify process model variables
   b) Identify values of variables of the process model
6) Identify feedback provided by PMV values

Model Element	CA Nr	Process Model Variable	Process Model Variable Values	Sensor or Controlled Process	Hazards
STI	5	sti_validation_status_ok	Yes / No	system_validation	H1, H3, H4
SiVES-S	12, 16, 20	sives_s_available_status_ok	Yes / No	system_operations	H1 to H4
	12, 20, 24	sives_s_authenticated_user	Yes / No	authentication	H1 to H4
SiVES-C	12, 15	sives_c_updated_in_virtual_stores	Yes / No	update_clients	H3.1, H3.2, H4.1
	15	sives_c_is_installed_and_updated	Yes / No	update_clients	H1, H3, H4
VMS	31	vms_available_status_ok	Yes / No	vms_operation	H2
Voter	24	voter_accepted_privacy_agreement	Yes / No	agreement	H1.1, H2 to H4

Analysis (Model the CS)

Modeling the Control Structure for Security (CS)

Variables Description

Model Element	Process Model Variable	Description
STI	sti_validation_status_ok	Indicates if system validation has been performed and SiVES is OK
SiVES-S	sives_s_available_status_ok	Indicates if SiVES-S is available
	sives_s_authenticated_user	Indicates if user is authenticated in SiVES-S
SiVES-C	sives_c_updated_in_virtual_store	Indicates if there is a new SiVES-C version (updating)
	sives_c_is_installed_and_updated	Indicates if SiVES-C is installed and updated
VMS	vms_available_status_ok	Indicates if VMS is available
Voter	voter_accepted_privacy_agreement	Indicates if voter accepted privacy agreement in SiVES-C

Analysis (Identify HCA) – Context Table

HAZARDS

H1: Voters unable to vote (reliability, availability and mission assurance issues)

H1.1: State that does not allow a legitimate voter to vote (to assure the mission)

H1.2: State that prevents the vote due to the system's unavailability and reliability issues (denial of service → availability and reliability)

H2: Voters unable to verify the vote (reliability, availability and mission assurance issues)

H2.1: State that does not allow a legitimate voter who voted to verify his/her own vote (to assure the mission)

H2.2: State that prevents to verify the vote due to the system's unavailability and reliability issues (denial of service → availability and reliability)

HAZARDS

H3: State that allows security violations (security issues)

H3.1: State that allows unauthorized access to private information (data, vote, etc.) (information disclosure → confidentiality)

H3.2: State that allows an unauthorized person to vote (spoofing → authentication and authorization)

H3.3: State that allows for undue alteration of the voter's vote (tampering → integrity)

H4: State that allows data privacy loss (privacy issues)

H4.1: State that allows information disclosure that links voter to vote (linkability → unlinkability)

H4.2: State that does not allow a voter to deny to whom he/she voted for (non-repudiation → plausible deniability)

Note #1: if all items in the same group of hazards belongs to the same analysis, the root hazard will be flagged to simplify the presentation. For instance, H1.1 and H1.2 would be simplified by H1.

Note #2: columns "Stopped too Soon / Applied too long / Wrong time/order" were omitted for better visualization, since they are not applicable in our example where all CA are discrete and not continuous, but column "Provided too late" can be used depending on the context in some cases.

CA Nr 01: Validate SiVES (TSE)	
Control Action provided	**Control Action not provided**
	H1.2, H2.2

CA Nr 02: Call for participation in mobile election (TSE)		
Control Action provided	**Control Action not provided**	**Control Action provided too late**
	H1.1	**H1.1**

CA Nr 03: Provide security and privacy guidelines to voter (TSE)		
Control Action provided	**Control Action not provided**	**Control Action provided too late**
	H3, H4	**H3, H4**

Analysis (Identify HCA) – Context Table

HAZARDS

H1: Voters unable to vote (reliability, availability and mission assurance issues)

H1.1: State that does not allow a legitimate voter to vote (to assure the mission)

H1.2: State that prevents the vote due to the system's unavailability and reliability issues (denial of service → availability and reliability)

H2: Voters unable to verify the vote (reliability, availability and mission assurance issues)

H2.1: State that does not allow a legitimate voter who voted to verify his/her own vote (to assure the mission)

H2.2: State that prevents to verify the vote due to the system's unavailability and reliability issues (denial of service → availability and reliability)

HAZARDS

H3: State that allows security violations (security issues)

H3.1: State that allows unauthorized access to private information (data, vote, etc.) (information disclosure → confidentiality)

H3.2: State that allows an unauthorized person to vote (spoofing → authentication and authorization)

H3.3: State that allows for undue alteration of the voter's vote (tampering → integrity)

H4: State that allows data privacy loss (privacy issues)

H4.1: State that allows information disclosure that links voter to vote (linkability → unlinkability)

H4.2: State that does not allow a voter to deny to whom he/she voted for (non-repudiation → plausible deniability)

CA Nr 04: Request changes of SiVES to STI (TSE)	
Control Action provided	**Control Action not provided**
	H1, H2, H3.2

CA Nr 05: Send SiVES-C installation package file to Virtual Stores (STI)		
Variables	**Control Action provided**	**Control Action not provided**
sti_validation_status_ok		
Yes		**H1.2, H3, H4**
No	**H1, H3, H4**	

Analysis (Identify HCA) – Context Table

HAZARDS

H1: Voters unable to vote (reliability, availability and mission assurance issues)

H1.1: State that does not allow a legitimate voter to vote (to assure the mission)

H1.2: State that prevents the vote due to the system's unavailability and reliability issues (denial of service → availability and reliability)

H2: Voters unable to verify the vote (reliability, availability and mission assurance issues)

H2.1: State that does not allow a legitimate voter who voted to verify his/her own vote (to assure the mission)

H2.2: State that prevents to verify the vote due to the system's unavailability and reliability issues (denial of service → availability and reliability)

HAZARDS

H3: State that allows security violations (security issues)

H3.1: State that allows unauthorized access to private information (data, vote, etc.) (information disclosure → confidentiality)

H3.2: State that allows an unauthorized person to vote (spoofing → authentication and authorization)

H3.3: State that allows for undue alteration of the voter's vote (tampering → integrity)

H4: State that allows data privacy loss (privacy issues)

H4.1: State that allows information disclosure that links voter to vote (linkability → unlinkability)

H4.2: State that does not allow a voter to deny to whom he/she voted for (non-repudiation → plausible deniability)

CA Nr 06: Follow security and privacy TSE guidelines (Voter)	
Control Action provided	**Control Action not provided**
	H3, H4

CA Nr 07: Install/update SiVES-C through the virtual store application when version is available (Voter)		
Control Action provided	**Control Action not provided**	**Control Action provided too late**
	H1	**H1**

CA Nr 08: Install SiVES-C from Virtual Store (Smartphone)	
Control Action provided	**Control Action not provided**
	H1.1

Analysis (Identify HCA) – Context Table

HAZARDS

H1: Voters unable to vote (reliability, availability and mission assurance issues)

H1.1: State that does not allow a legitimate voter to vote (to assure the mission)

H1.2: State that prevents the vote due to the system's unavailability and reliability issues (denial of service → availability and reliability)

H2: Voters unable to verify the vote (reliability, availability and mission assurance issues)

H2.1: State that does not allow a legitimate voter who voted to verify his/her own vote (to assure the mission)

H2.2: State that prevents to verify the vote due to the system's unavailability and reliability issues (denial of service → availability and reliability)

HAZARDS

H3: State that allows security violations (security issues)

H3.1: State that allows unauthorized access to private information (data, vote, etc.) (information disclosure → confidentiality)

H3.2: State that allows an unauthorized person to vote (spoofing → authentication and authorization)

H3.3: State that allows for undue alteration of the voter's vote (tampering → integrity)

H4: State that allows data privacy loss (privacy issues)

H4.1: State that allows information disclosure that links voter to vote (linkability → unlinkability)

H4.2: State that does not allow a voter to deny to whom he/she voted for (non-repudiation → plausible deniability)

CA Nr 09: Make and keep SiVES-S available (STI)	
Control Action provided	**Control Action not provided**
	H1

CA Nr 10: Provide biometric data (Voter)	
Control Action provided	**Control Action not provided**
	H1.1, H2.1

CA Nr 11: Accept the privacy agreement (Voter)	
Control Action provided	**Control Action not provided**
	H4

Analysis (Identify HCA) – Context Table

HAZARDS

H1: Voters unable to vote (reliability, availability and mission assurance issues)

H1.1: State that does not allow a legitimate voter to vote (to assure the mission)

H1.2: State that prevents the vote due to the system's unavailability and reliability issues (denial of service → availability and reliability)

H2: Voters unable to verify the vote (reliability, availability and mission assurance issues)

H2.1: State that does not allow a legitimate voter who voted to verify his/her own vote (to assure the mission)

H2.2: State that prevents to verify the vote due to the system's unavailability and reliability issues (denial of service → availability and reliability)

HAZARDS

H3: State that allows security violations (security issues)

H3.1: State that allows unauthorized access to private information (data, vote, etc.) (information disclosure → confidentiality)

H3.2: State that allows an unauthorized person to vote (spoofing → authentication and authorization)

H3.3: State that allows for undue alteration of the voter's vote (tampering → integrity)

H4: State that allows data privacy loss (privacy issues)

H4.1: State that allows information disclosure that links voter to vote (linkability → unlinkability)

H4.2: State that does not allow a voter to deny to whom he/she voted for (non-repudiation → plausible deniability)

CA Nr 12: Vote (Voter)					
Variables				**Control Action provided**	**Control Action not provided**
sives_s_available_status_ok	sives_s_authenticated_user	sives_c_is_installed_and_updated	voter_accepted_privacy_agreement		
Yes	Yes	Yes	Yes		**H3.1, H4.2**
Yes	Yes	Yes	No	**H3.2, H3.3, H4**	
Yes	Yes	No	Yes	**H3.2, H3.3, H4**	
Yes	Yes	No	No	**H3.2, H3.3, H4**	
Yes	No	Yes	Yes	**H3.2, H3.3, H4**	
Yes	No	Yes	No	**H3.2, H3.3, H4**	
Yes	No	No	Yes	**H3.2, H3.3, H4**	
Yes	No	No	No	**H3.2, H3.3, H4**	
No	Yes	Yes	Yes	**H3.2, H3.3, H4**	
No	Yes	Yes	No	**H3.2, H3.3, H4**	
No	Yes	No	Yes	**H3.2, H3.3, H4**	
No	Yes	No	No	**H3.2, H3.3, H4**	
No	No	Yes	Yes	**H3.2, H3.3, H4**	
No	No	Yes	No	**H3.2, H3.3, H4**	
No	No	No	Yes	**H3.2, H3.3, H4**	
No	No	No	No	**H3.2, H3.3, H4**	

Analysis (Identify HCA) – Context Table

HAZARDS

H1: Voters unable to vote (reliability, availability and mission assurance issues)

H1.1: State that does not allow a legitimate voter to vote (to assure the mission)

H1.2: State that prevents the vote due to the system's unavailability and reliability issues (denial of service → availability and reliability)

H2: Voters unable to verify the vote (reliability, availability and mission assurance issues)

H2.1: State that does not allow a legitimate voter who voted to verify his/her own vote (to assure the mission)

H2.2: State that prevents to verify the vote due to the system's unavailability and reliability issues (denial of service → availability and reliability)

HAZARDS

H3: State that allows security violations (security issues)

H3.1: State that allows unauthorized access to private information (data, vote, etc.) (information disclosure → confidentiality)

H3.2: State that allows an unauthorized person to vote (spoofing → authentication and authorization)

H3.3: State that allows for undue alteration of the voter's vote (tampering → integrity)

H4: State that allows data privacy loss (privacy issues)

H4.1: State that allows information disclosure that links voter to vote (linkability → unlinkability)

H4.2: State that does not allow a voter to deny to whom he/she voted for (non-repudiation → plausible deniability)

CA Nr 13: Receive voting confirmation (Voter)	
Control Action provided	**Control Action not provided**
	H1

CA Nr 14: Finalize session (Voter)		
Control Action provided	**Control Action not provided**	**Control Action provided too late**
	H3.1, H4	**H3.1, H3.3, H4**

CA Nr 15: Capture biometric data for authentication (SiVES-C and VMS)			
Variables		**Control Action provided**	**Control Action not provided**
sives_c_updated_in_virtual_stores	sives_c_is_installed_and_updated		
Yes	Yes		**H3.1, H4.1**
Yes	No	**H3.1, H3.2, H4.1**	
No	Yes	**H3.1, H3.2, H4.1**	
No	No	**H3.1, H3.2, H4.1**	

CA Nr 16: Send the user's biometric data to SiVES-S (SiVES-C and VMS)		
Variables	**Control Action provided**	**Control Action not provided**
sives_s_available_status_ok		
Yes		**H1.1, H4.1**
No	**H3.1, H3.2**	

Analysis (Identify HCA) – Context Table

HAZARDS

H1: Voters unable to vote (reliability, availability and mission assurance issues)

H1.1: State that does not allow a legitimate voter to vote (to assure the mission)

H1.2: State that prevents the vote due to the system's unavailability and reliability issues (denial of service → availability and reliability)

H2: Voters unable to verify the vote (reliability, availability and mission assurance issues)

H2.1: State that does not allow a legitimate voter who voted to verify his/her own vote (to assure the mission)

H2.2: State that prevents to verify the vote due to the system's unavailability and reliability issues (denial of service → availability and reliability)

HAZARDS

H3: State that allows security violations (security issues)

H3.1: State that allows unauthorized access to private information (data, vote, etc.) (information disclosure → confidentiality)

H3.2: State that allows an unauthorized person to vote (spoofing → authentication and authorization)

H3.3: State that allows for undue alteration of the voter's vote (tampering → integrity)

H4: State that allows data privacy loss (privacy issues)

H4.1: State that allows information disclosure that links voter to vote (linkability → unlinkability)

H4.2: State that does not allow a voter to deny to whom he/she voted for (non-repudiation → plausible deniability)

CA Nr 17: Display the SiVES-S response about user authentication (SiVES-C and VMS)	
Control Action provided	**Control Action not provided**
	H1.1

CA Nr 18: Offer the privacy agreement to the voter (SiVES-C and VMS)	
Control Action provided	**Control Action not provided**
	H3.1, H4.2

CA Nr 19: Send the required acceptance of the privacy agreement to SiVES-S (SiVES-C and VMS)	
Control Action provided	**Control Action not provided**
	H4

CA Nr 20: Send the voter's vote to SiVES-S (SiVES-C)			
Variables		**Control Action provided**	**Control Action not provided**
sives_s_authenticated_user	sives_s_available_status_ok		
Yes	Yes		**H1.1**
Yes	No	**H1.1**	
No	Yes	**H1.1, H3.1, H4.2**	
No	No	**H1.1, H3.1, H4.2**	

Analysis (Identify HCA) – Context Table

HAZARDS

H1: Voters unable to vote (reliability, availability and mission assurance issues)

H1.1: State that does not allow a legitimate voter to vote (to assure the mission)

H1.2: State that prevents the vote due to the system's unavailability and reliability issues (denial of service → availability and reliability)

H2: Voters unable to verify the vote (reliability, availability and mission assurance issues)

H2.1: State that does not allow a legitimate voter who voted to verify his/her own vote (to assure the mission)

H2.2: State that prevents to verify the vote due to the system's unavailability and reliability issues (denial of service → availability and reliability)

HAZARDS

H3: State that allows security violations (security issues)

H3.1: State that allows unauthorized access to private information (data, vote, etc.) (information disclosure → confidentiality)

H3.2: State that allows an unauthorized person to vote (spoofing → authentication and authorization)

H3.3: State that allows for undue alteration of the voter's vote (tampering → integrity)

H4: State that allows data privacy loss (privacy issues)

H4.1: State that allows information disclosure that links voter to vote (linkability → unlinkability)

H4.2: State that does not allow a voter to deny to whom he/she voted for (non-repudiation → plausible deniability)

CA Nr 21: Display and store voting confirmation or display error status (SiVES-C)	
Control Action provided	**Control Action not provided**
	H1.1, H3.2, H3.3, H4.1

CA Nr 22: Validate the biometric data received with the voter database (SiVES-S)	
Control Action provided	**Control Action not provided**
	H1.1, H3, H4

Analysis (Identify HCA) – Context Table

HAZARDS

H1: Voters unable to vote (reliability, availability and mission assurance issues)

H1.1: State that does not allow a legitimate voter to vote (to assure the mission)

H1.2: State that prevents the vote due to the system's unavailability and reliability issues (denial of service → availability and reliability)

H2: Voters unable to verify the vote (reliability, availability and mission assurance issues)

H2.1: State that does not allow a legitimate voter who voted to verify his/her own vote (to assure the mission)

H2.2: State that prevents to verify the vote due to the system's unavailability and reliability issues (denial of service → availability and reliability)

HAZARDS

H3: State that allows security violations (security issues)

H3.1: State that allows unauthorized access to private information (data, vote, etc.) (information disclosure → confidentiality)

H3.2: State that allows an unauthorized person to vote (spoofing → authentication and authorization)

H3.3: State that allows for undue alteration of the voter's vote (tampering → integrity)

H4: State that allows data privacy loss (privacy issues)

H4.1: State that allows information disclosure that links voter to vote (linkability → unlinkability)

H4.2: State that does not allow a voter to deny to whom he/she voted for (non-repudiation → plausible deniability)

CA Nr 23: Register the acceptance of the privacy agreement (SiVES-S)	
Control Action provided	**Control Action not provided**
	H2, H4

CA Nr 24: Receive and store the vote from SiVES-C (SiVES-S)			
Variables		**Control Action provided**	**Control Action not provided**
sives_s_authenticated_user	voter_accepted_privacy_agreement		
Yes	Yes		**H3.1, H3.3, H4.2**
Yes	No	**H1.1, H4.2**	
No	Yes	**H3.1, H3.3**	
No	No	**H3.1, H3.3, H4.2**	

CA Nr 25: Overwrite older vote in case of "revotation" (SiVES-S)	
Control Action provided	**Control Action not provided**
	H1.1, H3.3

Analysis (Identify HCA) – Context Table

HAZARDS

H1: Voters unable to vote (reliability, availability and mission assurance issues)

H1.1: State that does not allow a legitimate voter to vote (to assure the mission)

H1.2: State that prevents the vote due to the system's unavailability and reliability issues (denial of service → availability and reliability)

H2: Voters unable to verify the vote (reliability, availability and mission assurance issues)

H2.1: State that does not allow a legitimate voter who voted to verify his/her own vote (to assure the mission)

H2.2: State that prevents to verify the vote due to the system's unavailability and reliability issues (denial of service → availability and reliability)

HAZARDS

H3: State that allows security violations (security issues)

H3.1: State that allows unauthorized access to private information (data, vote, etc.) (information disclosure → confidentiality)

H3.2: State that allows an unauthorized person to vote (spoofing → authentication and authorization)

H3.3: State that allows for undue alteration of the voter's vote (tampering → integrity)

H4: State that allows data privacy loss (privacy issues)

H4.1: State that allows information disclosure that links voter to vote (linkability → unlinkability)

H4.2: State that does not allow a voter to deny to whom he/she voted for (non-repudiation → plausible deniability)

CA Nr 26: Finalize session in timeout case (SiVES-S)	
Control Action provided	**Control Action not provided**
	H3.1, H4

CA Nr 27: Make and keep VMS available to verification method (STI)	
Control Action provided	**Control Action not provided**
	H1.2, H2.2

CA Nr 28: Install and maintain verification infrastructure for the electoral office (STI)	
Control Action provided	**Control Action not provided**
	H2.2

Analysis (Identify HCA) – Context Table

HAZARDS

H1: Voters unable to vote (reliability, availability and mission assurance issues)

H1.1: State that does not allow a legitimate voter to vote (to assure the mission)

H1.2: State that prevents the vote due to the system's unavailability and reliability issues (denial of service → availability and reliability)

H2: Voters unable to verify the vote (reliability, availability and mission assurance issues)

H2.1: State that does not allow a legitimate voter who voted to verify his/her own vote (to assure the mission)

H2.2: State that prevents to verify the vote due to the system's unavailability and reliability issues (denial of service → availability and reliability)

HAZARDS

H3: State that allows security violations (security issues)

H3.1: State that allows unauthorized access to private information (data, vote, etc.) (information disclosure → confidentiality)

H3.2: State that allows an unauthorized person to vote (spoofing → authentication and authorization)

H3.3: State that allows for undue alteration of the voter's vote (tampering → integrity)

H4: State that allows data privacy loss (privacy issues)

H4.1: State that allows information disclosure that links voter to vote (linkability → unlinkability)

H4.2: State that does not allow a voter to deny to whom he/she voted for (non-repudiation → plausible deniability)

CA Nr 29: Register the verification request (SiVES-S)	
Control Action provided	**Control Action not provided**
	H3.1, H4

CA Nr 30: Provide voter's security and privacy (Electoral Office)	
Control Action provided	**Control Action not provided**
	H3.1, H3.3, H4

CA Nr 31: Provide verification service (Electoral Office)		
Variables	**Control Action provided**	**Control Action not provided**
vms_available_status_ok		
Yes		**H2**
No	**H2**	

Analysis (Identify HCA) – Context Table

HAZARDS

H1: Voters unable to vote (reliability, availability and mission assurance issues)

H1.1: State that does not allow a legitimate voter to vote (to assure the mission)

H1.2: State that prevents the vote due to the system's unavailability and reliability issues (denial of service → availability and reliability)

H2: Voters unable to verify the vote (reliability, availability and mission assurance issues)

H2.1: State that does not allow a legitimate voter who voted to verify his/her own vote (to assure the mission)

H2.2: State that prevents to verify the vote due to the system's unavailability and reliability issues (denial of service → availability and reliability)

HAZARDS

H3: State that allows security violations (security issues)

H3.1: State that allows unauthorized access to private information (data, vote, etc.) (information disclosure → confidentiality)

H3.2: State that allows an unauthorized person to vote (spoofing → authentication and authorization)

H3.3: State that allows for undue alteration of the voter's vote (tampering → integrity)

H4: State that allows data privacy loss (privacy issues)

H4.1: State that allows information disclosure that links voter to vote (linkability → unlinkability)

H4.2: State that does not allow a voter to deny to whom he/she voted for (non-repudiation → plausible deniability)

CA Nr 32: Verify the vote (Voter)				
Variables			**Control Action provided**	**Control Action not provided**
sives_s_available_status_ok	sives_s_authenticated_user	voter_accepted_privacy_agreement		
Yes	Yes	Yes		**H2**
Yes	Yes	No	**H2, H3.1, H4**	
Yes	No	Yes	**H2, H3.1, H4**	
Yes	No	No	**H2, H3.1, H4**	
No	Yes	Yes	**H2, H3.1, H4**	
No	Yes	No	**H2, H3.1, H4**	
No	No	Yes	**H2, H3.1, H4**	
No	No	No	**H2, H3.1, H4**	

CA Nr 33: Request vote (VMS)	
Control Action provided	**Control Action not provided**
	H2

Analysis (Define controller constraints) – Hazardous Control Actions and Controller Constraints

CA Nr 01: Validate SiVES (TSE)	
Hazardous Control Actions	**Controller Constraints**
TSE not provided validate SiVES (**not provide**)	TSE must provided validate SiVES

Analysis (Define controller constraints) – Hazardous Control Actions and Controller Constraints

CA Nr 02: Call for participation in mobile election (TSE)	
Hazardous Control Actions	**Controller Constraints**
TSE not provided call for participation in mobile election (**not provided**)	TSE must provide call for participation in mobile election
TSE provided call for participation in mobile election too late (**too late**)	TSE must not provided call for participation in mobile election too late

Analysis (Define controller constraints) – Hazardous Control Actions and Controller Constraints

CA Nr 03: Provide security and privacy guidelines to voter (TSE)	
Hazardous Control Actions	**Controller Constraints**
TSE not provide provide security and privacy guidelines to voter (**not provided**)	TSE must provide provide security and privacy guidelines to voter
TSE provide provide security and privacy guidelines to voter too late (**too late**)	TSE must not provide provide security and privacy guidelines to voter too late

Analysis (Define controller constraints) – Hazardous Control Actions and Controller Constraints

CA Nr 04: Request changes of SiVES to STI (TSE)	
Hazardous Control Actions	**Controller Constraints**
TSE not provided request changes of SiVES to STI (**not provided**)	TSE must request changes of SiVES to STI

Analysis (Define controller constraints) – Hazardous Control Actions and Controller Constraints

CA Nr 05: Send SiVES-C installation package file to Virtual Stores (STI)	
Hazardous Control Actions	**Controller Constraints**
STI not provided send SiVES-C installation package file to Virtual Stores when sti_validation_status_ok is yes (**not provided**)	STI must provide send SiVES-C installation package file to Virtual Stores when sti_validation_status_ok is yes
STI provided send SiVES-C installation package file to Virtual Stores when sti_validation_status_ok is no (**provided**)	STI must not provide send SiVES-C installation package file to Virtual Stores when sti_validation_status_ok is no

Analysis (Define controller constraints) – Hazardous Control Actions and Controller Constraints

CA Nr 06: Follow security and privacy TSE guidelines (Voter)	
Hazardous Control Actions	**Controller Constraints**
Voter not provide follow security and privacy TSE guidelines (**not provided**)	Voter must provide follow security and privacy TSE guidelines

Analysis (Define controller constraints) – Hazardous Control Actions and Controller Constraints

CA Nr 07: Install/update SiVES-C through the virtual store application when version is available (Voter)	
Hazardous Control Actions	**Controller Constraints**
Voter not provided install/update SiVES-C through the virtual store application when version is available (**not provided**)	Voter must provide install/update SiVES-C through the virtual store application when version is available
Voter provided install/update SiVES-C through the virtual store application when version is available too late (**too late**)	Voter must not provided install/update SiVES-C through the virtual store application when version is available too late

Analysis (Define controller constraints) – Hazardous Control Actions and Controller Constraints

CA Nr 08: Install SiVES-C from Virtual Store (Smartphone)	
Hazardous Control Actions	**Controller Constraints**
Voter not provided install SiVES-C from Virtual Store (**not provided**)	Voter must provide install SiVES-C from Virtual Store

Analysis (Define controller constraints) – Hazardous Control Actions and Controller Constraints

CA Nr 09: Make and keep SiVES-S available (STI)	
Hazardous Control Actions	**Controller Constraints**
STI not provided make and keep SiVES-S available (**not provided**)	STI must provide make and keep SiVES-S available

Analysis (Define controller constraints) – Hazardous Control Actions and Controller Constraints

CA Nr 10: Provide biometric data (Voter)	
Hazardous Control Actions	**Controller Constraints**
Voter not provided provide biometric data (**not provided**)	Voter must provided provide biometric data

Analysis (Define controller constraints) – Hazardous Control Actions and Controller Constraints

CA Nr 11: Accept the privacy agreement (Voter)	
Hazardous Control Actions	**Controller Constraints**
Voter not provided accept the privacy agreement (**not provided**)	Voter must provide accept the privacy agreement

Analysis (Define controller constraints) – Hazardous Control Actions and Controller Constraints

CA Nr 12: Vote (Voter)	
Hazardous Control Actions	**Controller Constraints**
Voter not provided vote when sives_s_available_status_ok is yes and sives_s_authenticated_user is yes and sives_c_is_installed_and_updated is yes and voter_accepted_privacy_agreement is yes (**not provided**)	Voter must provided vote when sives_s_available_status_ok is yes and sives_s_authenticated_user is yes and sives_c_is_installed_and_updated is yes and voter_accepted_privacy_agreement is yes
Voter provided vote when sives_s_available_status_ok is yes and sives_s_authenticated_user is yes and sives_c_is_installed_and_updated is yes and voter_accepted_privacy_agreement is no (**provided**)	Voter must not provided vote when sives_s_available_status_ok is yes and sives_s_authenticated_user is yes and sives_c_is_installed_and_updated is yes and voter_accepted_privacy_agreement is no
Voter provided vote when sives_s_available_status_ok is yes and sives_s_authenticated_user is yes and sives_c_is_installed_and_updated is no and voter_accepted_privacy_agreement is yes (**provided**)	Voter must not provided vote when sives_s_available_status_ok is yes and sives_s_authenticated_user is yes and sives_c_is_installed_and_updated is no and voter_accepted_privacy_agreement is yes
Voter provided vote when sives_s_available_status_ok is yes and sives_s_authenticated_user is yes and sives_c_is_installed_and_updated is no and voter_accepted_privacy_agreement is no (**provided**)	Voter must not provided vote when sives_s_available_status_ok is yes and sives_s_authenticated_user is yes and sives_c_is_installed_and_updated is no and voter_accepted_privacy_agreement is no
Voter provided vote when sives_s_available_status_ok is yes and sives_s_authenticated_user is no and sives_c_is_installed_and_updated is yes and voter_accepted_privacy_agreement is yes (**provided**)	Voter must not provided vote when sives_s_available_status_ok is yes and sives_s_authenticated_user is no and sives_c_is_installed_and_updated is yes and voter_accepted_privacy_agreement is yes
Voter provided vote when sives_s_available_status_ok is yes and sives_s_authenticated_user is no and sives_c_is_installed_and_updated is yes and voter_accepted_privacy_agreement is no (**provided**)	Voter must not provided vote when sives_s_available_status_ok is yes and sives_s_authenticated_user is no and sives_c_is_installed_and_updated is yes and voter_accepted_privacy_agreement is no
Voter provided vote when sives_s_available_status_ok is yes and sives_s_authenticated_user is no and sives_c_is_installed_and_updated is no and voter_accepted_privacy_agreement is yes (**provided**)	Voter must not provided vote when sives_s_available_status_ok is yes and sives_s_authenticated_user is no and sives_c_is_installed_and_updated is no and voter_accepted_privacy_agreement is yes

Analysis (Define controller constraints) – Hazardous Control Actions and Controller Constraints

CA Nr 12: Vote (Voter)	
Hazardous Control Actions	**Controller Constraints**
Voter provided vote when sives_s_available_status_ok is yes and sives_s_authenticated_user is no and sives_c_is_installed_and_updated is no and voter_accepted_privacy_agreement is no (**provided**)	Voter must not provided vote when sives_s_available_status_ok is yes and sives_s_authenticated_user is no and sives_c_is_installed_and_updated is no and voter_accepted_privacy_agreement is no
Voter provided vote when sives_s_available_status_ok is no and sives_s_authenticated_user is yes and sives_c_is_installed_and_updated is yes and voter_accepted_privacy_agreement is yes (**provided**)	Voter must not provided vote when sives_s_available_status_ok is no and sives_s_authenticated_user is yes and sives_c_is_installed_and_updated is yes and voter_accepted_privacy_agreement is yes
Voter provided vote when sives_s_available_status_ok is no and sives_s_authenticated_user is yes and sives_c_is_installed_and_updated is yes and voter_accepted_privacy_agreement is no (**provided**)	Voter must not provided vote when sives_s_available_status_ok is no and sives_s_authenticated_user is yes and sives_c_is_installed_and_updated is yes and voter_accepted_privacy_agreement is no
Voter provided vote when sives_s_available_status_ok is no and sives_s_authenticated_user is yes and sives_c_is_installed_and_updated is no and voter_accepted_privacy_agreement is yes (**provided**)	Voter must not provided vote when sives_s_available_status_ok is no and sives_s_authenticated_user is yes and sives_c_is_installed_and_updated is no and voter_accepted_privacy_agreement is yes
Voter provided vote when sives_s_available_status_ok is no and sives_s_authenticated_user is yes and sives_c_is_installed_and_updated is no and voter_accepted_privacy_agreement is no (**provided**)	Voter must not provided vote when sives_s_available_status_ok is no and sives_s_authenticated_user is yes and sives_c_is_installed_and_updated is no and voter_accepted_privacy_agreement is no
Voter provided vote when sives_s_available_status_ok is no and sives_s_authenticated_user is no and sives_c_is_installed_and_updated is yes and voter_accepted_privacy_agreement is yes (**provided**)	Voter must not provided vote when sives_s_available_status_ok is no and sives_s_authenticated_user is no and sives_c_is_installed_and_updated is yes and voter_accepted_privacy_agreement is yes
Voter provided vote when sives_s_available_status_ok is no and sives_s_authenticated_user is no and sives_c_is_installed_and_updated is yes and voter_accepted_privacy_agreement is no (**provided**)	Voter must not provided vote when sives_s_available_status_ok is no and sives_s_authenticated_user is no and sives_c_is_installed_and_updated is yes and voter_accepted_privacy_agreement is no

Analysis (Define controller constraints) – Hazardous Control Actions and Controller Constraints

CA Nr 12: Vote (Voter)	
Hazardous Control Actions	**Controller Constraints**
Voter provided vote when sives_s_available_status_ok is no and sives_s_authenticated_user is no and sives_c_is_installed_and_updated is no and voter_accepted_privacy_agreement is yes (**provided**)	Voter must not provided vote when sives_s_available_status_ok is no and sives_s_authenticated_user is no and sives_c_is_installed_and_updated is no and voter_accepted_privacy_agreement is yes
Voter provided vote when sives_s_available_status_ok is no and sives_s_authenticated_user is no and sives_c_is_installed_and_updated is no and voter_accepted_privacy_agreement is no (**provided**)	Voter must not provided vote when sives_s_available_status_ok is no and sives_s_authenticated_user is no and sives_c_is_installed_and_updated is no and voter_accepted_privacy_agreement is no

Analysis (Define controller constraints) – Hazardous Control Actions and Controller Constraints

CA Nr 13: Receive voting confirmation (Voter)	
Hazardous Control Actions	**Controller Constraints**
Voter not provide receive voting confirmation (**not provided**)	Voter must provide receive voting confirmation

Analysis (Define controller constraints) – Hazardous Control Actions and Controller Constraints

CA Nr 14: Finalize session (Voter)	
Hazardous Control Actions	**Controller Constraints**
Voter not provide finalize session (**not provided**)	Voter must provide finalize session
Voter provide finalize session too late (**too late**)	Voter must not provide finalize session too late

Analysis (Define controller constraints) – Hazardous Control Actions and Controller Constraints

CA Nr 15: Capture biometric data for authentication (SiVES-C and VMS)	
Hazardous Control Actions	**Controller Constraints**
SiVES-C and VMS not provided capture biometric data for authentication when sives_c_updated_in_virtual_stores is yes and sives_c_is_installed_and_updated is yes (**not provided**)	SiVES-C and VMS must provide capture biometric data for authentication when sives_c_updated_in_virtual_stores is yes and sives_c_is_installed_and_updated is yes
SiVES-C and VMS provided capture biometric data for authentication when sives_c_updated_in_virtual_stores is yes and sives_c_is_installed_and_updated is no (**provided**)	SiVES-C and VMS must not provide capture biometric data for authentication when sives_c_updated_in_virtual_stores is yes and sives_c_is_installed_and_updated is no
SiVES-C and VMS provided capture biometric data for authentication when sives_c_updated_in_virtual_stores is no and sives_c_is_installed_and_updated is yes (**provided**)	SiVES-C and VMS must not provide capture biometric data for authentication when sives_c_updated_in_virtual_stores is no and client_is_updated is yes
SiVES-C and VMS provided capture biometric data for authentication when sives_c_updated_in_virtual_stores is no and sives_c_is_installed_and_updated is no (**provided**)	SiVES-C and VMS must not provide capture biometric data for authentication when sives_c_updated_in_virtual_stores is no and sives_c_is_installed_and_updated is no

Analysis (Define controller constraints) – Hazardous Control Actions and Controller Constraints

CA Nr 16: Send the user's biometric data to SiVES-S (SiVES-C and VMS)	
Hazardous Control Actions	**Controller Constraints**
SiVES-C and VMS not provided send the user's biometric data to SiVES-S when sives_s_available_status_ok is yes (**not provided**)	SiVES-C and VMS must provide send the user's biometric data to SiVES-S when sives_s_available_status_ok is yes
SiVES-C and VMS provided send the user's biometric data to SiVES-S when sives_s_available_status_ok is no (**provided**)	SiVES-C and VMS must not provide send the user's biometric data to SiVES-S when sives_s_available_status_ok is no

Analysis (Define controller constraints) – Hazardous Control Actions and Controller Constraints

CA Nr 17: Display the SiVES-S response about user authentication (SiVES-C and VMS)	
Hazardous Control Actions	**Controller Constraints**
SiVES-C and VMS not provided display the SiVES-S response about user authentication (**not provided**)	SiVES-C and VMS must provide display the SiVES-S response about user authentication

Analysis (Define controller constraints) – Hazardous Control Actions and Controller Constraints

CA Nr 18: Offer the privacy agreement to the voter (SiVES-C and VMS)	
Hazardous Control Actions	**Controller Constraints**
SiVES-C and VMS not provided offer the confidentiality agreement to the voter (**not provided**)	SiVES-C and VMS must provide offer the confidentiality agreement to the

Analysis (Define controller constraints) – Hazardous Control Actions and Controller Constraints

CA Nr 19: Send the required acceptance of the privacy agreement to SiVES-S (SiVES-C and VMS)	
Hazardous Control Actions	**Controller Constraints**
SiVES-C and VMS not provide send the required acceptance of the privacy agreement to SiVES-S (**not provided**)	SiVES-C and VMS must provide send the required acceptance of the privacy agreement to SiVES-S

Analysis (Define controller constraints) – Hazardous Control Actions and Controller Constraints

CA Nr 20: Send the voter's vote to SiVES-S (SiVES-C)	
Hazardous Control Actions	**Controller Constraints**
SiVES-C not provide send the voter's vote to SiVES-S when sives_s_authenticated_user is no and sives_s_available_status_ok is no (provided)_s_available_status_ok is yes (**not provided**)	SiVES-C must provide send the voter's vote to SiVES-S when sives_s_authenticated_user is no and sives_s_available_status_ok is no (provided)_s_available_status_ok is yes
SiVES-C provided send the voter's vote to SiVES-S when sives_s_authenticated_user is no and sives_s_available_status_ok is no (provided)_s_available_status_ok is no (**provided**)	SiVES-C must not provide send the voter's vote to SiVES-S when sives_s_authenticated_user is no and sives_s_available_status_ok is no (provided)_s_available_status_ok is no
SiVES-C provided send the voter's vote to SiVES-S when sives_s_authenticated_user is no and sives_s_available_status_ok is yes (**provided**)	SiVES-C must not provide send the voter's vote to SiVES-S when sives_s_authenticated_user is no and sives_s_available_status_ok is no (provided)_s_available_status_ok is yes
SiVES-C provided send the voter's vote to SiVES-S when sives_s_authenticated_user is no and sives_s_available_status_ok is no (**provided**)	SiVES-C must not provide send the voter's vote to SiVES-S when sives_s_authenticated_user is no and sives_s_available_status_ok is no (provided)_s_available_status_ok is no

Analysis (Define controller constraints) – Hazardous Control Actions and Controller Constraints

CA Nr 21: Display and store voting confirmation or display error status (SiVES-C)	
Hazardous Control Actions	**Controller Constraints**
SiVES-C not provide display and store voting confirmation or display error status (**not provided**)	SiVES-C must provide display and store voting confirmation or display error status

Analysis (Define controller constraints) – Hazardous Control Actions and Controller Constraints

CA Nr 22: Validate the biometric data received with the voter database (SiVES-S)	
Hazardous Control Actions	**Controller Constraints**
SiVES-S not provided validate the biometric data received with the voter database (**not provided**)	SiVES-S must provide validate the biometric data received with the voter database

Analysis (Define controller constraints) – Hazardous Control Actions and Controller Constraints

CA Nr 23: Register the acceptance of the privacy agreement (SiVES-S)	
Hazardous Control Actions	**Controller Constraints**
SiVES-S not provided register the acceptance of the privacy agreement (**not provided**)	SiVES-S must provide register the acceptance of the privacy agreement

Analysis (Define controller constraints) – Hazardous Control Actions and Controller Constraints

CA Nr 24: Receive and store the vote from SiVES-C (SiVES-S)	
Hazardous Control Actions	**Controller Constraints**
SiVES-S not provide receive and store the vote from SiVES-C when sives_s_authenticated_user is yes and voter_accepted_privacy_agreement is yes (**not provided**)	SiVES-S must provide receive and store the vote from SiVES-C when voter_accepted_privacy_agreement is yes
SiVES-S receive and store the vote from SiVES-C when sives_s_authenticated_user is yes and voter_accepted_privacy_agreement is no (**provided**)	SiVES-S must not receive and store the vote from SiVES-C when sives_s_authenticated_user is yes and voter_accepted_privacy_agreement is no
SiVES-S receive and store the vote from SiVES-C when sives_s_authenticated_user is no and voter_accepted_privacy_agreement is yes (**provided**)	SiVES-S must not receive and store the vote from SiVES-C when sives_s_authenticated_user is no and voter_accepted_privacy_agreement is yes
SiVES-S receive and store the vote from SiVES-C when sives_s_authenticated_user is no and voter_accepted_privacy_agreement is no (**provided**)	SiVES-S must not receive and store the vote from SiVES-C when sives_s_authenticated_user is no and voter_accepted_privacy_agreement is no

Analysis (Define controller constraints) – Hazardous Control Actions and Controller Constraints

CA Nr 25: Overwrite older vote in case of “revotation” (SiVES-S)	
Hazardous Control Actions	**Controller Constraints**
SiVES-S not provide overwrite older vote in case of “revotation” when SiVES-S received the vote (**not provided**)	SiVES-S must provide overwrite older vote in case of “revotation” when SiVES-S received the vote

Analysis (Define controller constraints) – Hazardous Control Actions and Controller Constraints

CA Nr 26: Finalize session in timeout case (SiVES-S)	
Hazardous Control Actions	**Controller Constraints**
SiVES-S not provide finalize session in timeout case (**not provided**)	SiVES-S must provide finalize session in timeout case

Analysis (Define controller constraints) – Hazardous Control Actions and Controller Constraints

CA Nr 27: Make and keep VMS available to verification method (STI)	
Hazardous Control Actions	**Controller Constraints**
STI not provided make and keep VMS available to verification method (**not provided**)	STI must provide make and keep VMS available to verification method

Analysis (Define controller constraints) – Hazardous Control Actions and Controller Constraints

CA Nr 28: Install and maintain verification infrastructure for the electoral office (STI)	
Hazardous Control Actions	**Controller Constraints**
STI not provided install and maintain verification infrastructure for the electoral office (**not provided**)	STI must provide install and maintain verification infrastructure for the electoral office

Analysis (Define controller constraints) – Hazardous Control Actions and Controller Constraints

CA Nr 29: Register the verification request (SiVES-S)	
Hazardous Control Actions	**Controller Constraints**
SiVES-S not provided register the verification request (**not provided**)	SiVES-S must provide register the verification request

Analysis (Define controller constraints) – Hazardous Control Actions and Controller Constraints

CA Nr 30: Provide voter's security and privacy (Electoral Office)	
Hazardous Control Actions	**Controller Constraints**
Electoral Office not provided voter's security and privacy (**not provided**)	Electoral Office must provide voter's security and privacy

Analysis (Define controller constraints) – Hazardous Control Actions and Controller Constraints

CA Nr 31: Provide verification service (Electoral Office)	
Hazardous Control Actions	**Controller Constraints**
Electoral Office not provided verification service when vms_available_status_ok is yes (**not provided**)	Electoral Office must provide verification servisse when vms_available_status_ok is yes
Electoral Office provided verification service when vms_available_status_ok is no (**provided**)	Electoral Office must not provide verification servisse when vms_available_status_ok is no

Analysis (Define controller constraints) – Hazardous Control Actions and Controller Constraints

CA Nr 32: Verify the vote (Voter)	
Hazardous Control Actions	**Controller Constraints**
Voter provided verify the vote when sives_s_available_status_ok is yes and sives_s_authenticated_user is yes and voter_accepted_privacy_agreement is yes (**not provided**)	Voter must provided verify the vote when sives_s_available_status_ok is yes and sives_s_authenticated_user is yes and voter_accepted_privacy_agreement is yes
Voter provided verify the vote when sives_s_available_status_ok is yes and sives_s_authenticated_user is yes and voter_accepted_privacy_agreement is no (**provided**)	Voter must not provided verify the vote when sives_s_available_status_ok is yes and sives_s_authenticated_user is yes and voter_accepted_privacy_agreement is no
Voter provided verify the vote when sives_s_available_status_ok is yes and sives_s_authenticated_user is no and voter_accepted_privacy_agreement is yes (**provided**)	Voter must not provided verify the vote when sives_s_available_status_ok is yes and sives_s_authenticated_user is no and voter_accepted_privacy_agreement is yes
Voter provided verify the vote when sives_s_available_status_ok is yes and sives_s_authenticated_user is no and voter_accepted_privacy_agreement is no (**provided**)	Voter must not provided verify the vote when sives_s_available_status_ok is yes and sives_s_authenticated_user is no and voter_accepted_privacy_agreement is no
Voter provided verify the vote when sives_s_available_status_ok is no and sives_s_authenticated_user is yes and voter_accepted_privacy_agreement is yes (**provided**)	Voter must not provided verify the vote when sives_s_available_status_ok is no and sives_s_authenticated_user is yes and voter_accepted_privacy_agreement is yes
Voter provided verify the vote when sives_s_available_status_ok is no and sives_s_authenticated_user is yes and voter_accepted_privacy_agreement is no (**provided**)	Voter must not provided verify the vote when sives_s_available_status_ok is no and sives_s_authenticated_user is yes and voter_accepted_privacy_agreement is no
Voter provided verify the vote when sives_s_available_status_ok is no and sives_s_authenticated_user is no and voter_accepted_privacy_agreement is yes (**provided**)	Voter must not provided verify the vote when sives_s_available_status_ok is no and sives_s_authenticated_user is no and voter_accepted_privacy_agreement is yes
Voter provided verify the vote when sives_s_available_status_ok is no and sives_s_authenticated_user is no and voter_accepted_privacy_agreement is no (**provided**)	Voter must not provided verify the vote when sives_s_available_status_ok is no and sives_s_authenticated_user is no and voter_accepted_privacy_agreement is no

Analysis (Define controller constraints) – Hazardous Control Actions and Controller Constraints

CA Nr 33: Request vote (VMS)	
Hazardous Control Actions	**Controller Constraints**
VMS not provide request vote (**not provided**)	VMS must provide request vote

Steps 1, 2 and 3 – Summary

Overview Data Analysis – General STPA Results up to Step 3 (*Privacy domain was removed*)

INFORMATIONS	QUANTITY
Unacceptable Losses	3
Hazards	7
Constraints	8
Control Actions	28
Hazardous Control Actions	63
Controller Constraints	63

Process to identify the security requirements - Overview

The process to identify the security requirements is:

- Execute steps 1, 2 and 3
- Execute activities 4.1 and 4.2 from STPA Step 4
- Map model elements and obtain the DFD (DIEFD) from CS (Task 4.3.1)
- Identify threats and vulnerabilities in DIEFD (STRIDE Analysis) (Task 4.3.2)
- Identify scenarios (Task 4.3.3)
- Consolidate Losses (Activity 4.4): for each HCA, verify which 3-tuple can be a causal factor. If it can be, generate a requirement (recommendation) with redundancy check (NEW and REP states)

Execute activities 4.1 and 4.2 from STPA Step 4

NOTE: To test the extension of the model, we have adopted it for the sake of simplicity of this analysis and not to make this presentation very much extensive, we will only analyze one Hazardous Control Action for a single Control Action.

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)				
Hazardous Control Action: SiVES-C not provide send the voter's vote to SiVES-S when sives_s_authenticated_user is no and sives_s_available_status_ok is no (provided)				
Group 1 (Right Side): hazardous control action provided or safe control action required but not provided (issued)				
Nr	**Scenarios**	**Associated Causal Factors**	**Requirements**	**Rationales**
1	SiVES-C receives the wrong value from SiVES-S (voting confirmation)	Failure in the communication between SiVES-C and SiVES-S.	The communication between SiVES-C and SiVES-S must be improved.	---
2	Value of SiVES-S (voting confirmation) is missing	Failure in the communication between SiVES-C and SiVES-S.	The communication between SiVES-C and SiVES-S must be improved.	---
3	An incorrect algorithm was designed	Algorithm wrong or incomplete or lack of knowledge of the system.	The algorithm must be revised and tested after each change to reduce errors.	Simulations of the system can help to validate the algorithm.

Execute activities 4.1 and 4.2 from STPA Step 4

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)				
Hazardous Control Action: SiVES-C not provide send the voter's vote to SiVES-S when sives_s_authenticated_user is no and sives_s_available_status_ok is no (provided)				
Group 1 (Right Side): hazardous control action provided or safe control action required but not provided (issued)				
Nr	**Scenarios**	**Associated Causal Factors**	**Requirements**	**Rationales**
4	Algorithm ineffective, unsafe or incomplete after process changes.	Algorithm was not updated to support changes of the process.	Algorithm must be updated, revised and tested after each change in the process to reduce errors.	Algorithm must be revised and adapted to support the process changes.
5	Algorithm updated incorrectly.	Flaw in the modifications or algorithm was not updated to support the modifications.	After each modification in the algorithm, it must be revised and tested to reduce errors.	Algorithm should be updated properly for each change.
6	Current state of the process model is inconsistent, incorrect or incomplete.	Feedback of emergency missing or with wrong value.	Process model in the SiVES-S Controlled Process must be consistent with the SiVES-S (voting confirmation) and external system status.	Not Applicable
7	Temporary obstruction not allow the reading of the SiVES-S (voting confirmation)	Obstruction for observing; Mean obstructed.	Alternative way to read the SiVES-S (voting confirmation) should be considered	Not Applicable

Execute activities 4.1 and 4.2 from STPA Step 4

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)				
Hazardous Control Action: SiVES-C not provide send the voter's vote to SiVES-S when sives_s_authenticated_user is no and sives_s_available_status_ok is no (provided)				
Group 1 (Right Side): hazardous control action provided or safe control action required but not provided (issued)				
Nr	**Scenarios**	**Associated Causal Factors**	**Requirements**	**Rationales**
8	Current state of the SiVES-S (voting confirmation) cannot be read accurately.	Obstruction for observing; Mean obstructed; Poor environment conditions or; Accuracy property is not guaranteed.	Most capable sensor or alternative way to read the SiVES-S (user authenticated and accepted privacy agreement) should be considered.	SiVES-S (voting confirmation) Sensor may not be calibrated
9	SiVES-S (voting confirmation) cannot be read by the SiVES-S (voting confirmation) Sensor	Reading errors; Variations in the SiVES-S (voting confirmation) or; Precision and sensitivity properties are not guaranteed.	The correct type of sensor must be chosen according to the controlled process.	Not Applicable
10	SiVES-S (voting confirmation) Sensor cannot get the status of the SiVES-S	Failure in the SiVES-S (voting confirmation) Sensor.	The SiVES-S (voting confirmation) Sensor must be maintained periodically.	Reliability analysis can reduce the failures.
11	Feedback delays to reach the SiVES-C Controller	Limitations in the communication protocol or problem in the communication mean (Wire or Wireless)	Communication between SiVES-S Controlled Process and SiVES-S (voting confirmation) Sensor must be improved.	Alternative communication means can be considered.

Execute activities 4.1 and 4.2 from STPA Step 4

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)				
Hazardous Control Action: SiVES-C not provide send the voter's vote to SiVES-S when sives_s_authenticated_user is no and sives_s_available_status_ok is no (provided)				
Group 2 (Left Side): control action improperly executed or not executed				
Nr	**Scenarios**	**Associated Causal Factors**	**Requirements**	**Rationales**
12	SiVES-S Controlled Process does not provide the control action or issued an incorrect	Problems in the process model and/or control algorithms.	Process model in SiVES-S Controlled Process must be the same in the SiVES-S and the control	Not applicable
13	The system components do not perform their functions.	Failure in one or more components of the system.	Ongoing STPA analysis must be done in order to cover each change in the system.	Reliability analysis can be done for small components introduced in the system. Complex components must have their own STPA analysis.
14	SiVES-S affected by natural or man made disasters.	Depends of the disaster.	Some disasters cabe mitigated	Not applicable
15	The issued control action delays to be enforced by the Actuator.	Failure in the Actuator, electric failure or temporary loss of power	The Actuator must be maintained periodically.	Reliability analysis can reduce the failures.
16	SiVES-S Controlled Process does not provide the control action or issued an incorrect.	Problems in the process model and/or control algorithms.	Process model in SiVES-S Controlled Process must be the same in the SiVES-S and the control	Not applicable

Execute activities 4.1 and 4.2 from STPA Step 4

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)				
Hazardous Control Action: SiVES-C not provide send the voter's vote to SiVES-S when sives_s_authenticated_user is no and sives_s_available_status_ok is no (provided)				
Group 2 (Left Side): control action improperly executed or not executed				
Nr	**Scenarios**	**Associated Causal Factors**	**Requirements**	**Rationales**
17	The system components do not perform their functions.	Failure in one or more components of the system.	Ongoing STPA analysis must be done in order to cover each change in the system.	Reliability analysis can be done for small components introduced in the system. Complex components must have their own STPA analysis.

Steps 1, 2 and 3 – Summary

Overview Data Analysis – General STPA Results up to Step 3 (*Privacy domain was removed*)

INFORMATIONS	QUANTITY
Unacceptable Losses	3
Hazards	7
Constraints	8
Control Actions	28
Hazardous Control Actions	63
Controller Constraints	63

Activities 4.1 and 4.2 – Summary

Results to **one** Control Action (CA Nr 20) and to **one** Hazardous Control Action

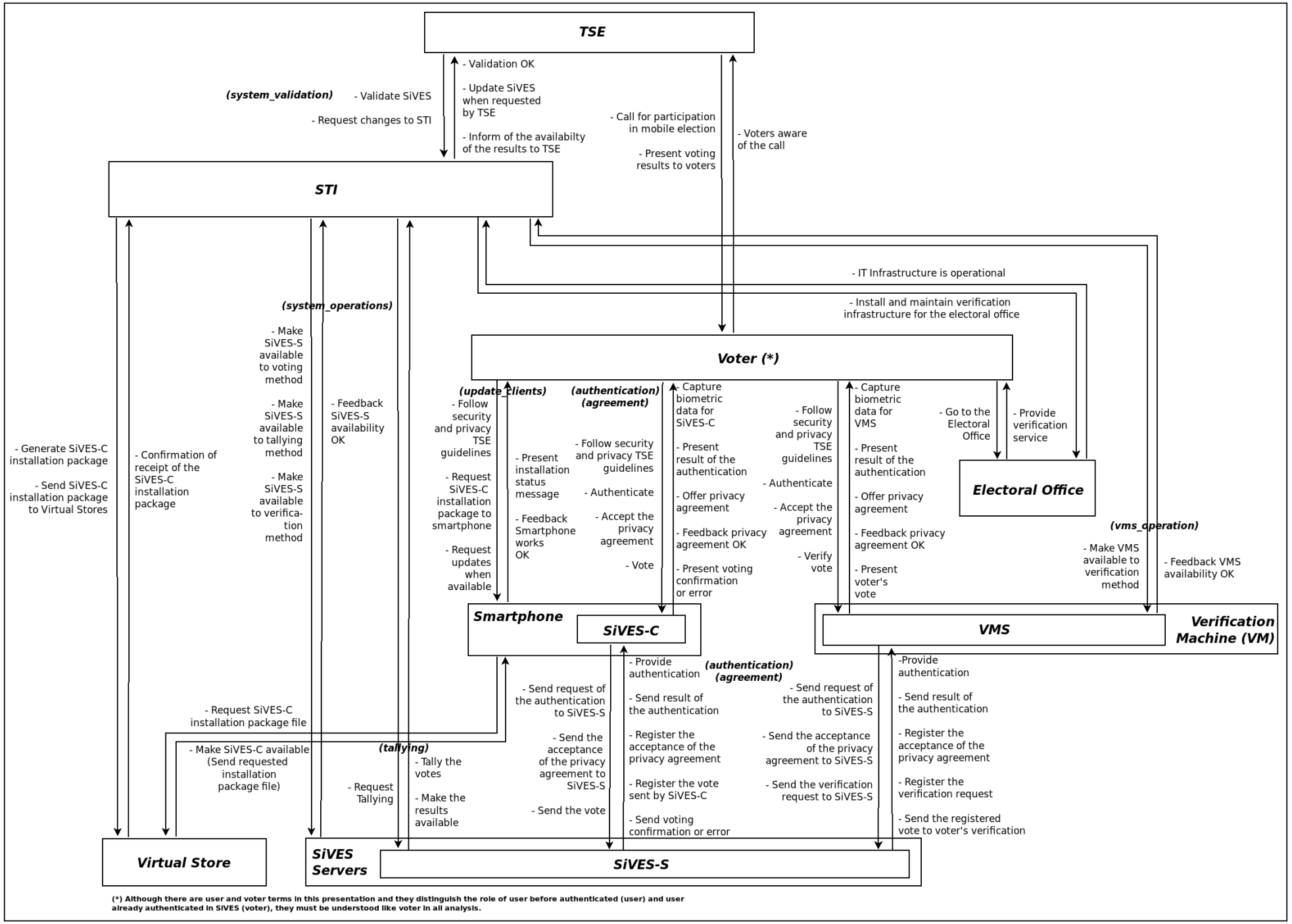
INFORMATIONS	QUANTITY
Scenarios (Sce)	17
Requirements (Req)	17

Process to identify the security requirements - Overview

The process to identify the security requirements is:

- Execute steps 1, 2 and 3
- Execute activities 4.1 and 4.2 from STPA Step 4
- Map model elements and obtain the DFD (DIEFD) from CS (Task 4.3.1)
- Identify threats and vulnerabilities in DIEFD (STRIDE Analysis) (Task 4.3.2)
- Identify scenarios (Task 4.3.3)
- Consolidate Losses (Activity 4.4): for each HCA, verify which 3-tuple can be a causal factor. If it can be, generate a requirement (recommendation) with redundancy check (NEW and REP states)

Control Structure (CS)



Model Elements

1) TSE
2) STI
3) Voter
4) Virtual Store
5) Smartphone
6) SiVES-C (mobile client)
7) SiVES Servers (hardware)
8) SiVES-S (server application)
9) Electoral Office
10) Verification Machine
11) Verification Machine Software (VMS)

STRIDE

STRIDE

Several papers show that STRIDE is not a standardized methodology and, because of this, there are some approaches to this type of analysis. In the diagram presented, we see a 5-step approach.

STRIDE PROCESS

1. Identify Components (Assets): define system elements
2. Plot DFD: visualize its funcionalities within or external to the system
3. Analyze threat scenarios: identify threats in DFD
4. Identify vulnerabilities: identify causes
5. Plan mitigation strategies: determine mitigation strategies based on the discovered vulnerabilities

STRIDE

Elements of DFD

- External Entity
- Process
- Data Flow
- Data Store

All the elements are focused on data!

Interaction between DFD elements and STRIDE

Element	S	T	R	I	D	E
External Entity	X		X			
Process	X	X	X	X	X	X
Data Store		X	X	X	X	
Data Flow		X		X	X	

STPA Extension with STRIDE

We will adopt as a starting point for this extension the CS of STPA

To extend them it is necessary to map concepts between the models. We will start with STRIDE (security).

Mapping Model Elements from CS to DFD

"→" means "maps to"

Controller → Process (may include Data Store) or External Entity

- Algorithm → Process
- Process Model → Data Store
- Links between Algorithm and Process Model → Data Flow (generally not an issue)

Control Action (to Actuator/Controlled Process) → Data/Information Flow

Actuator → Process (exceptionally may include Data Store and have links)

Link between Actuator and Process Model → Data/Information/Energy Flow

Mapping Model Elements from CS to DFD

Controlled Process → Process (may include Data Store and have links)

Input → Data/Information/Energy Flow and External Entity

Output → Data/Information/Energy Flow and External Entity

State → Data/Information/Energy Flow

Sensor → Process (exceptionally may include Data Store and have links)

Feedback → Data/Information Flow

External Communication → Data/Information Flow and External Entity

Mapping Model Elements from CS to DFD

Other control input to Controller/Controlled Process → Data/Information/Energy Flow

Environmental Disturbances → Energy Flow

Mapping Model Elements from CS to DFD

We have to consider other forms of flow: information and energy!

The mapping is generally straightforward; however, there are two main mapping issues:

- Determine when the controller is a process or an external entity.
- Set the Trust the Boundaries of the system

In order to illustrate the mapping and solve these issues, we use an example: Glucose Control System with Smartphone.

Mapping Model Elements from CS to DFD

Processes and Data Stores can be detailed (broken down). Iteration may be required for the Controlled Process.

Trust boundary intersect data flow and indicate point where an attacker can exploit.

- Processes interacting in a network in general have trust boundaries.

Context Diagram is a high-level diagram that models the entire system and its main components. We think that is the level for STPA analysis.

A more appropriate name for DFD would be DIEFD (Data/Information/Energy Flow Diagram)

DIEFD Elements mapped to CS STPA

Elements		S	T	R	I	D	E
DIEFD	STPA						
External Entity	Controller (Algorithm) Input Output External Communication Other control input to Controller/Controlled Process Environmental Disturbances	X		X			
Process	Controller Actuator Controlled Process Sensor	X	X	X	X	X	X
Data Store	Controller (Process Model) Actuator Controlled Process Sensor		X	X	X	X	
Data Flow	Control Action (to Actuator/Controlled Process) Link between Actuator and Process Model Input Output Sensing Feedback External Communication Other control input to Controller/Controlled Process Environmental Disturbances		X		X	X	

Map model elements and obtain DFD (DIEFD) from CS – Example

Mapping of the Electronic Voting System by Smartphone (SiVES) (CS → DIEFD)

TSE (Controller) → External Entity

STI (Controller or Actuator) → External Entity or Process

Voter (Controller) → External Entity

Virtual Stores (EE) → Data/Information Flow and External Entity

Smartphone (Actuator) → Process

SiVES-C (Controller) → Process

NOTE: We have define whether the elements are processes or external entities. In order to do that, we identify the trust boundaries. We will use our example to illustrate our ideas.

Map model elements and obtain DFD (DIEFD) from CS – Example

Mapping of the Electronic Voting System by Smartphone (SiVES) (CS → DIEFD)

SiVES Servers (Actuator) → Process

SiVES-S (Controlled Process) → Process and Data Store

Electoral Office (Controller) → External Entity

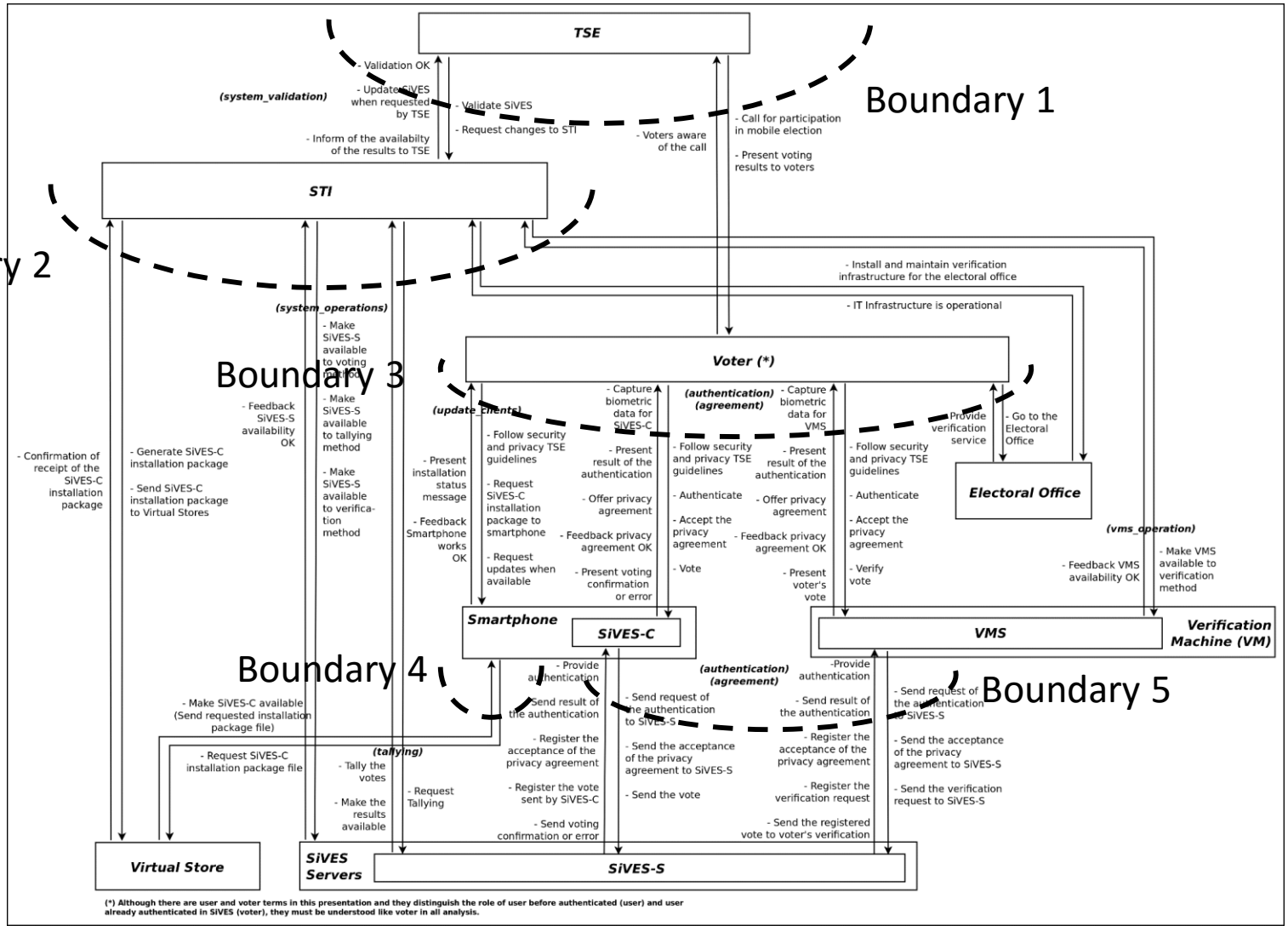
Verification Machine (Actuator) → Process

VMS (Controller) → Process or External Entity

NOTE: We have define whether the elements are processes or external entities. In order to do that, we identify the trust boundaries. We will use our example to illustrate our ideas.

Map model elements and obtain DFD (DIEFD) from CS – Example

In order to determine if an STAMP element is an External Entity, it is of help to define the Trust Boundaries. We can do that in the CS.



Map model elements and obtain DFD (DIEFD) from CS – Example Trust Boundaries

We identify trust boundaries for the links.

We identify 7 Trust Boundaries:

- Boundary Nr 01 where attackers can exploit the link between the TSE and Voter and TSE and STI.
- Boundary Nr 02 where attackers can exploit the link among the STI and Virtual Stores, SiVES Servers SiVES-S, Electoral Office and VMS.
- Boundary Nr 03 where attackers can exploit the link among the Voter and Smartphone, SiVES-C, VMS and Electoral Office.
- Boundary Nr 04 where attackers can exploit the link between the Smartphone and Virtual Stores.

Map model elements and obtain DFD (DIEFD) from CS – Example Trust Boundaries

- Boundary Nr 05 where attackers can exploit the link between the SiVES-C and SiVES-S.

- Boundary Nr 06 where attackers can exploit the link between the VMS and SiVES-S.

We consider that the Boundaries Nr 01, 03 and 04 are safe and secure due to be relationship between internal system components and voter (Voter) or between internal components of electoral justice (TSE, STI, Electoral Office). Boundary 02 is safe and secure, except the link between STI and Virtual Stores.

We consider that the Boundary Nr 05 and the link between Virtual Stores and STI of the Boundary Nr 02 exploitable by the attacker. This means that attackers can exploit links that reach these boundaries.

Map model elements and obtain DFD (DIEFD) from CS – Example Trust Boundaries

We assume that:

- the links Voter – TSE, Voter – Smartphone, Voter – Verification Machine, Voter – Electoral Office are NOT vulnerable.

- the links TSE – STI, STI – Electoral Office, STI – SiVES Servers, STI – SiVES-S and STI – VMS are NOT vulnerable

This means that Trust Boundaries do NOT define a total order, but just a partial one.

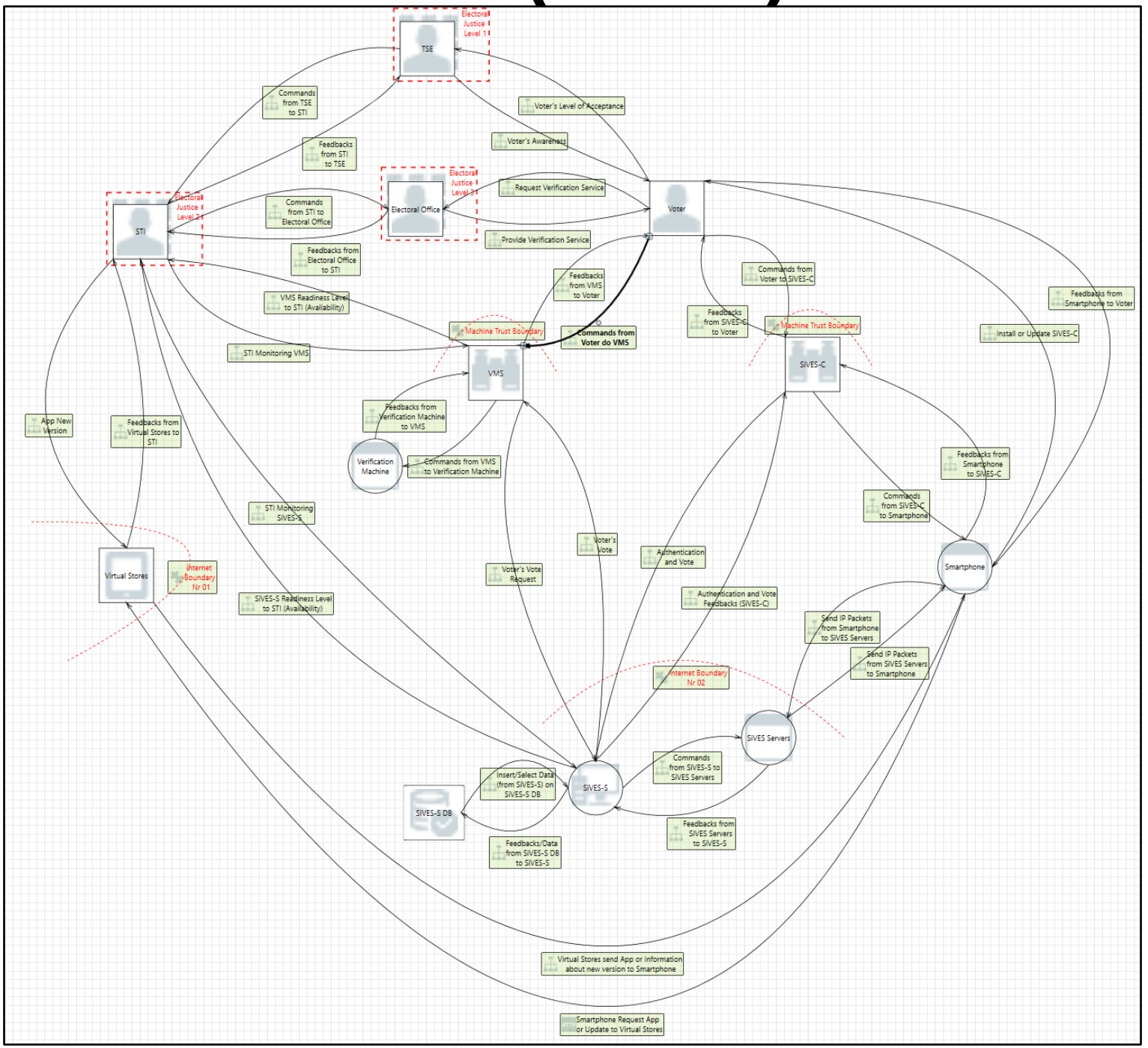
We may consider zones of trust and their ordering.

Since STAMP is hierarchical, we may consider some ordering of zones of trust! It looks Partial Ordering (not Total Ordering)

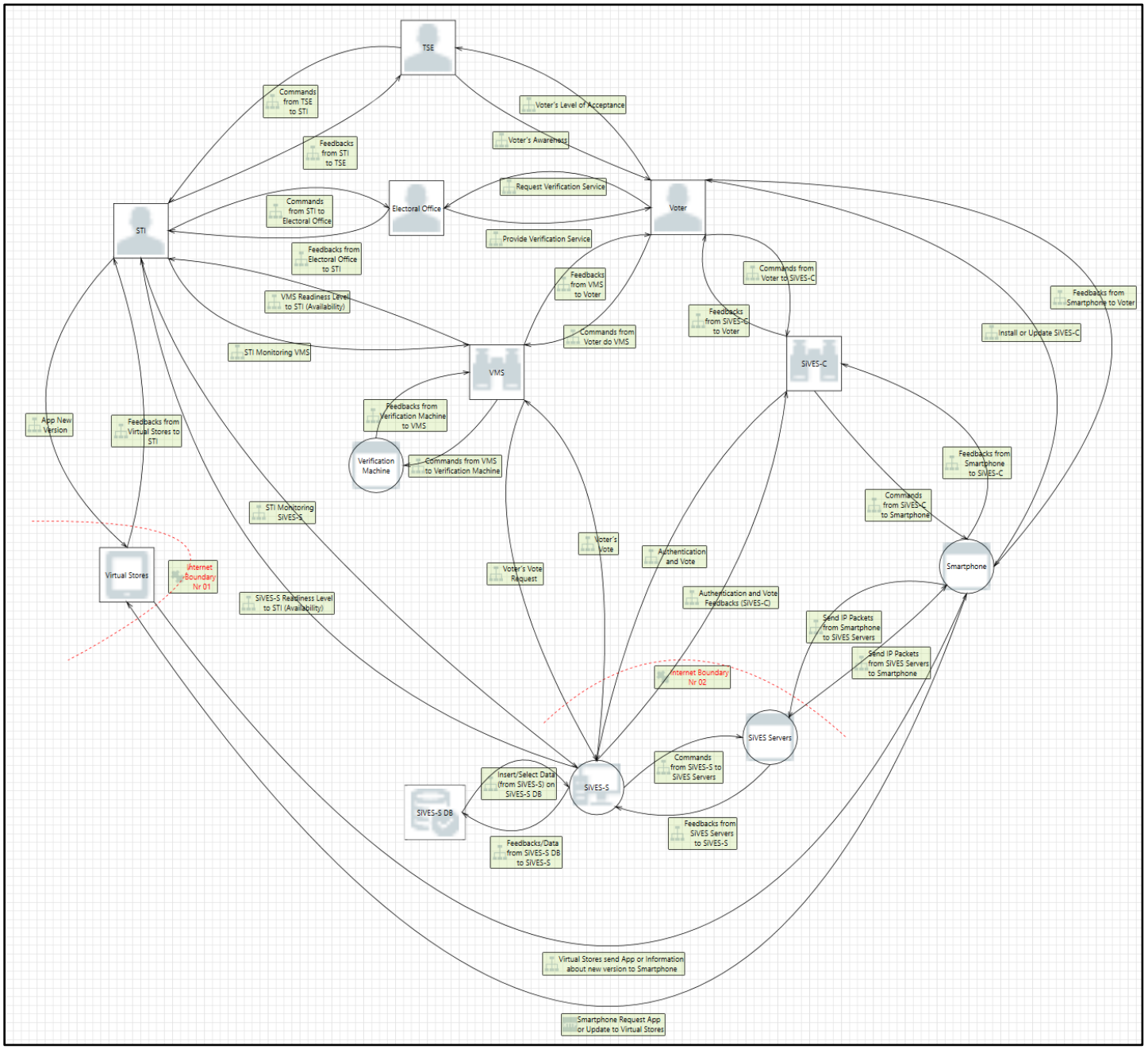
DIEFD Elements mapped from CS STPA – Example

Elements			S	T	R	I	D	E
DIEFD	STPA	Example (SiVES)						
External Entity	Controller Controller Controller External Comm Controller	TSE STI Electoral Office Virtual Stores Voter	X		X			
Process	Actuator Controller Actuator Controlled Process Actuator Controller	Smartphone SiVES-C SiVES Servers SiVES-S Verification Machine VMS	X	X	X	X	X	X
Data Store	Controlled Process	SiVES-S		X	X	X	X	
Data Flow	External Comm	Virtual Stores SiVES-C → SiVES-S (Link) VMS → SiVES-S (Link)		X		X	X	

DFD (DIEFD)


Electoral Justice Level 1
TSE
Commands from TSE to STI
Feedbacks from STI to TSE
Voter's Level of Acceptance
Voter's Awareness
Electoral Justice Level 2
STI
Commands from STI to Electoral Office
Feedbacks from Electoral Office to STI
Electoral Justice Level 3
Electoral Office
Request Verification Service
Provide Verification Service
Voter
VMS Readiness Level to STI (Availability)
STI Monitoring VMS
Machine Trust Boundary
VMS
Feedbacks from VMS to Voter
Commands from Voter do VMS
Commands from Voter to SIVES-C
Feedbacks from SIVES-C to Voter
Machine Trust Boundary
SIVES-C
Feedbacks from Smartphone to Voter
Install or Update SIVES-C
App New Version
Feedbacks from Virtual Stores to STI
Feedbacks from Verification Machine to VMS
Verification Machine
Commands from VMS to Verification Machine
Feedbacks from Smartphone to SIVES-C
Commands from SIVES-C to Smartphone
STI Monitoring SIVES-S
Voter's Vote
Authentication and Vote
Smartphone
Virtual Stores
Internet Boundary Nr 01
Voter's Vote Request
Authentication and Vote Feedbacks (SIVES-C)
SIVES-S Readiness Level to STI (Availability)
Send IP Packets from Smartphone to SIVES Servers
Send IP Packets from SIVES Servers to Smartphone
Internet Boundary Nr 02
SIVES Servers
Commands from SIVES-S to SIVES Servers
Insert/Select Data (from SIVES-S) on SIVES-S DB
SIVES-S
SIVES-S DB
Feedbacks from SIVES Servers to SIVES-S
Feedbacks/Data from SIVES-S DB to SIVES-S
Virtual Stores send App or Information about new version to Smartphone
Smartphone Request App or Update to Virtual Stores

DFD (DIEFD) considering Boundaries Nr 02 and 05 removing boundaries assumed like NOT vulnerables



Process to identify the security requirements - Overview

The process to identify the security requirements is:

- Execute steps 1, 2 and 3
- Execute activities 4.1 and 4.2 from STPA Step 4
- Map model elements and obtain the DFD (DIEFD) from CS (Task 4.3.1)
- Identify threats and vulnerabilities in DIEFD (STRIDE Analysis) (Task 4.3.2)
- Identify scenarios (Task 4.3.3)
- Consolidate Losses (Activity 4.4): for each HCA, verify which 3-tuple can be a causal factor. If it can be, generate a requirement (recommendation) with redundancy check (NEW and REP states)

Identify threats and vulnerabilities in DIEFD (Execute STRIDE Analysis)

See the STRIDE analysis in file "**SiVES-without-not-vulnerable-boundaries4.pdf**" that follows along with this presentation

NOTE: The Microsoft Threat Modeling Tool 2016 has a bug on report generation. The priorities is not considered. Because of this, we manually change the priorities in the PDF to depict the analysis made in the tool.

Process to identify the security requirements - Overview

The process to identify the security requirements is:

- Execute steps 1, 2 and 3
- Execute activities 4.1 and 4.2 from STPA Step 4
- Map model elements and obtain the DFD (DIEFD) from CS (Task 4.3.1)
- Identify threats and vulnerabilities in DIEFD (STRIDE Analysis) (Task 4.3.2)
- Identify scenarios (Task 4.3.3)
- Consolidate Losses (Activity 4.4): for each HCA, verify which 3-tuple can be a causal factor. If it can be, generate a requirement (recommendation) with redundancy check (NEW and REP states)

Identify Scenarios
Identify a possible 3-tuple (causal factor) from STRIDE
OVERVIEW THREATS AGAINST INTERACTIONS AMONG ELEMENTS

Nr	Interaction	Elements	Nr	Threats
1	Commands from SiVES-C to Smartphone (DF)	SiVES-C (Proc) and Smartphone (Proc)	1	Spoofing the SiVES-C External Entity
			2	Elevation Using Impersonation
2	Commands from SiVES-S to SiVES Servers (DF)	SiVES-S (Proc) and SiVES Servers (Proc)	3	Elevation Using Impersonation
3	Feedbacks from SiVES-S to SiVES-C (DF)	SiVES-C (Proc) and SiVES-S (Proc)	4	Spoofing of the SiVES-C External Destination Entity
			5	External Entity SiVES-C Potentially Denies Receiving Data
			6	Data Flow Generic Is Potentially Interrupted
4	App New Version (DF)	STI (EE) and Virtual Stores (EE)	7	External Entity Virtual Stores Potentially Denies Receiving Data
			8	Data Flow Generic Is Potentially Interrupted
5	Vote (DF)	SiVES-S (Proc) and SiVES-C (Proc)	9	Spoofing the SiVES-S Process
			10	Spoofing the SiVES-C External Entity
			11	Potential Lack of Input Validation for SiVES-S
			12	Cross Site Scripting
			13	Potential Data Repudiation by SiVES-S
			14	Data Flow Sniffing
			15	Potential Process Crash or Stop for SiVES-S
			16	Data Flow Generic Is Potentially Interrupted

Identify Scenarios
Identify a possible 3-tuple (causal factor) from STRIDE
OVERVIEW THREATS AGAINST INTERACTIONS AMONG ELEMENTS

Nr	Interaction	Elements	Nr	Threats
5	Vote (DF)	SiVES-S (Proc) and SiVES-C (Proc)	17	Elevation Using Impersonation
			18	SiVES-S May be Subject to Elevation of Privilege Using Remote Code Execution
			19	Elevation by Changing the Execution Flow in SiVES-S
			20	Cross Site Request Forgery
6	Commands from VMS to Verification Machine (DF)	Verification Machine (Proc) and VMS (Proc)	21	Spoofing the SiVES-C External Entity
			22	Elevation Using Impersonation
7	Feedbacks from SiVES Servers to SiVES-S (DF)	SiVES-S (Proc) and SiVES Servers (Proc)	23	Cross Site Scripting
			24	Elevation Using Impersonation
8	Feedbacks from Virtual Stores to STI (DF)	STI (EE) and Virtual Stores (EE)	25	External Entity STI Potentially Denies Receiving Data
			26	Data Flow Generic Is Potentially Interrupted
9	Feedbacks/Data from SiVES-S DB to SiVES-S (DF)	SiVES-S DB (DS) and SiVES-S (Proc)	27	Spoofing of Destination Data Store SQL Database
			28	Potential SQL Injection Vulnerability for SQL Database
			29	Potential Excessive Resource Consumption for SiVES-S or SQL Database
			30	Weak Credential Storage

Identify Scenarios
Identify a possible 3-tuple (causal factor) from STRIDE
OVERVIEW THREATS AGAINST INTERACTIONS AMONG ELEMENTS

Nr	Interaction	Elements	Nr	Threats
10	Insert/Select Data (from SiVES-S) on SiVES-S DB (DF)	SiVES-S DB (DS) and SiVES-S (Proc)	31	Spoofing of Source Data Store SQL Database
			32	Cross Site Scripting
			33	Persistent Cross Site Scripting
			34	Weak Access Control for a Resource
11	Install or Update SiVES-C (DF)	Voter (EE) and Smartphone (Proc)	35	Elevation Using Impersonation
			36	Spoofing the Voter External Entity
12	Send IP Packets from SiVES Servers to Smartphone (DF)	SiVES Servers (Proc) and Smartphone (Proc)	37	Elevation Using Impersonation
			38	Spoofing the SiVES Servers Process
			39	Spoofing the Smartphone Process
			40	Potential Data Repudiation by Smartphone
			41	Potential Process Crash or Stop for Smartphone
			42	Data Flow Send IP Packets from SiVES Servers to Smartphone Is Potentially Interrupted
			43	Smartphone May be Subject to Elevation of Privilege Using Remote Code Execution
			44	Elevation by Changing the Execution Flow in Smartphone
			45	Potential Lack of Input Validation for Smartphone
			46	Data Flow Sniffing

Identify Scenarios
Identify a possible 3-tuple (causal factor) from STRIDE
OVERVIEW THREATS AGAINST INTERACTIONS AMONG ELEMENTS

Nr	Interaction	Elements	Nr	Threats
13	Send IP Packets from Smartphone to SiVES Servers (DF)	SiVES Servers (Proc) and Smartphone (Proc)	47	Elevation Using Impersonation
			48	Spoofing the Smartphone Process
			49	Spoofing the SiVES Servers Process
			50	Potential Data Repudiation by SiVES Servers
			51	Potential Process Crash or Stop for SiVES Servers
			52	Data Flow Send IP Packets from Smartphone to SiVES Servers Is Potentially Interrupted
			53	SiVES Servers May be Subject to Elevation of Privilege Using Remote Code Execution
			54	Elevation by Changing the Execution Flow in SiVES Servers
			55	Potential Lack of Input Validation for SiVES Servers
			56	Data Flow Sniffing
14	Smartphone Request App or Update to Virtual Stores (DF)	Virtual Stores (Proc) and Smartphone (Proc)	57	Data Flow Generic Is Potentially Interrupted
			58	External Entity Virtual Stores Potentially Denies Receiving Data
			59	Spoofing of the Virtual Stores External Destination Entity
15	STI Monitoring SiVES-S (DF)	STI (EE) and SiVES-S (Proc)	60	Spoofing the STI External Entity
			61	Cross Site Scripting

Identify Scenarios
Identify a possible 3-tuple (causal factor) from STRIDE
OVERVIEW THREATS AGAINST INTERACTIONS AMONG ELEMENTS

Nr	Interaction	Elements	Nr	Threats
15	STI Monitoring SiVES-S (DF)	STI (EE) and SiVES-S (Proc)	62	Elevation Using Impersonation
16	Virtual Stores send App or Information about new version to Smartphone (DF)	Virtual Stores (Proc) and Smartphone (Proc)	63	Elevation by Changing the Execution Flow in Smartphone
			64	Smartphone May be Subject to Elevation of Privilege Using Remote Code Execution
			65	Elevation Using Impersonation
			66	Data Flow Generic Is Potentially Interrupted
			67	Potential Process Crash or Stop for Smartphone
			68	Data Flow Sniffing
			69	Potential Data Repudiation by Smartphone
			70	Potential Lack of Input Validation for Smartphone
			71	Spoofing the Virtual Stores External Entity
			72	Spoofing the Smartphone Process
17	Voter´s Level of Acceptance (DF)	TSE (EE) and Voter (EE)	73	Authenticated Data Flow Compromised
			74	Spoofing the SiVES-S Process
			75	Spoofing the VMS External Entity
			76	Potential Lack of Input Validation for SiVES-S
			77	Cross Site Scripting

Identify Scenarios
Identify a possible 3-tuple (causal factor) from STRIDE
OVERVIEW THREATS AGAINST INTERACTIONS AMONG ELEMENTS

Nr	Interaction	Elements	Nr	Threats
17	Voter´s Level of Acceptance (DF)	TSE (EE) and Voter (EE)	78	Potential Data Repudiation by SiVES-S
			79	Data Flow Sniffing
			80	Potential Process Crash or Stop for SiVES-S
			81	Data Flow Generic Is Potentially Interrupted
			82	Elevation Using Impersonation
			83	SiVES-S May be Subject to Elevation of Privilege Using Remote Code Execution
			84	Elevation by Changing the Execution Flow in SiVES-S
			85	Cross Site Request Forgery
18	Voter´s Vote (DF)	VMS (Proc) and SiVES-S (Proc)	86	Spoofing of the VMS External Destination Entity
			87	External Entity VMS Potentially Denies Receiving Data
			88	Data Flow Generic Is Potentially Interrupted

Identify Scenarios
Identify a possible 3-tuple (causal factor) from STRIDE

OVERVIEW THREATS DIRECTLY AGAINST ELEMENTS

Elements
TSE (EE)
STI (EE)
Electoral Office (EE)
Virtual Stores (EE)
Voter (EE)
Smartphone (Proc)
SiVES-C (Proc)
SiVES Servers (Proc)
SiVES-S (Proc)
Verification Machine (Proc)
VMS (Proc)

Identify Scenarios
Identify a possible 3-tuple (causal factor) from STRIDE

Nr	Interaction	Elements
1	Commands from SiVES-C to Smartphone (DF)	SiVES-C (Proc) and Smartphone (Proc)

Threat: 1. Spoofing the SiVES-C External Entity			
Category: Spoofing			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
SiVES-C may be spoofed by an attacker and this may lead to unauthorized access to Smartphone. Consider using a standard authentication mechanism to identify the external entity.	There is no user authenation on SiVES-S from SiVES-C	The system shall provide user authentication	
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them	

Threat: 2. Elevation Using Impersonation			
Category: Elevation of Privilege			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
Smartphone may be able to impersonate the context of SiVES-C in order to gain additional privilege.	Incorrect or insecure configuration	System configuration must be revised and hardened	
	Lack of training (competence) of system administrators, led to incorrect or insecure configurations	Administrators must be trained and have knowledge recycled regularly	
	There is no user authenation on SiVES-S from SiVES-C	The system shall provide user authentication	
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them	

Identify Scenarios
Identify a possible 3-tuple (causal factor) from STRIDE

Nr	Interaction	Elements
2	Commands from SiVES-S to SiVES Servers (DF)	SiVES-S (Proc) and SiVES Servers (Proc)

Threat: 3. Elevation Using Impersonation			
Category: Elevation of Privilege			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
SiVES Servers may be able to impersonate the context of SiVES-S in order to gain additional privilege.	Incorrect or insecure configuration	System configuration must be revised and hardened	
	Lack of training (competence) of system administrators, led to incorrect or insecure configurations	Administrators must be trained and have knowledge recycled regularly	
	There is no user authenation on SiVES-S from SiVES-C	The system shall provide user authentication	
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them	

Identify Scenarios
Identify a possible 3-tuple (causal factor) from STRIDE

Nr	Interaction	Elements
3	Feedbacks from SiVES-S to SiVES-C (DF)	SiVES-C (Proc) and SiVES-S (Proc)

Threat: 4. Spoofing of the SiVES-C External Destination Entity			
Category: Spoofing			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
SiVES-C may be spoofed by an attacker and this may lead to information disclosure by SIVES-S	There is no user authenation on SiVES-S from SiVES-C	The system shall provide user authentication	
	No cliente to server authentication and vice versa	The system shall provide authentication for both directions	
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them	

Threat: 5. External Entity SiVES-C Potentially Denies Receiving Data			
Category: Repudiation			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
SiVES-C claims that it did not receive data from a process on the other side of the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.	Inadequate or inexistent service control and logs	Provide logs and auditing to ensure non-repudiation	
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them	

Identify Scenarios
Identify a possible 3-tuple (causal factor) from STRIDE

Nr	Interaction	Elements
3	Feedbacks from SiVES-S to SiVES-C (DF)	SiVES-C (Proc) and SiVES-S (Proc)

Threat: 6. Data Flow Generic Is Potentially Interrupted			
Category: Denial Of Service			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
An external agent interrupts data flowing across a trust boundary in either direction.	Inadequate or insufficient resources allow denial of service	The system must have means to avoid DoS attack, like redundancy.	
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them	

Identify Scenarios
Identify a possible 3-tuple (causal factor) from STRIDE

Nr	Interaction	Elements
4	App New Version (DF)	STI (EE) and Virtual Stores (EE)

Threat: 7. External Entity Virtual Stores Potentially Denies Receiving Data			
Category: Repudiation			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
Virtual Stores claims that it did not receive data from a process on the other side of the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.	Inadequate or inexistent service control and logs	Provide logs and auditing to ensure non-repudiation	
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them	

Threat: 8. Data Flow Generic Is Potentially Interrupted			
Category: Denial Of Service			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
An external agent interrupts data flowing across a trust boundary in either direction.	Inadequate or insufficient resources allow denial of service	The system must have means to avoid DoS attack, like redundancy.	
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them	

Identify Scenarios
Identify a possible 3-tuple (causal factor) from STRIDE

Nr	Interaction	Elements
5	Vote (DF)	SiVES-S (Proc) and SiVES-C (Proc)

Threat: 9. Spoofing the SiVES-S Process			
Category: Spoofing			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
SiVES-S may be spoofed by an attacker and this may lead to information disclosure by SiVES-C. Consider using a standard authentication mechanism to identify the destination process.	There is no user authenation on SiVES-S from SiVES-C	The system shall provide user authentication	
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them	

Threat: 10. Spoofing the SiVES-C External Entity			
Category: Spoofing			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
SiVES-C may be spoofed by an attacker and this may lead to unauthorized access to SiVES-S. Consider using a standard authentication mechanism to identify the external entity.	There is no user authenation on SiVES-S from SiVES-C	The system shall provide user authentication	
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them	

Identify Scenarios
Identify a possible 3-tuple (causal factor) from STRIDE

Nr	Interaction	Elements
5	Vote (DF)	SiVES-S (Proc) and SiVES-C (Proc)

Threat: 11. Potential Lack of Input Validation for SiVES-S			
Category: Tampering			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
Data flowing across Vote may be tampered with by an attacker. This may lead to a denial of service attack against SiVES-S or an elevation of privilege attack against SiVES-S or an information disclosure by SiVES-S.	SiVES-S inputs is not validated	The input shall be validated	
	Connection failure between SiVES-C and SiVES-S	Since the connection is made using Internet, nothing can be made. We assume that TCP handles the failure	
	Intentional Tampering of data by external agent	The system shall provide message integrity check mechanism	
	SiVES-C output is not validated	The output shall be validated	
	Incorrect or insecure SiVES-S configuration	The SiVES-S configuration shall be reviewed and hardened.	
	Lack of knowledge of system administrators that leads to incorrect or insecure settings	The system administrators shall be regularly recycled	
	Presence of software bugs in SiVES-S and/or SiVES-C	The software shall be continuously tested and maintained.	

Identify Scenarios
Identify a possible 3-tuple (causal factor) from STRIDE

Nr	Interaction	Elements
5	Vote (DF)	SiVES-S (Proc) and SiVES-C (Proc)

Threat: 12. Cross Site Scripting			
Category: Tampering			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
The server 'SiVES-S' could be a subject to a cross-site scripting attack because it does not sanitize untrusted input.	Inputs are not being validated	The input shall be validated	
	Data injection modifies system behavior	The system shall have the latest update of antimalware and shall remove the malware	

Threat: 13. Potential Data Repudiation by SiVES-S			
Category: Repudiation			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
SiVES-S claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.	Inadequate or inexistent service control and logs	Provide logs and auditing to ensure non-repudiation	
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them	

Identify Scenarios
Identify a possible 3-tuple (causal factor) from STRIDE

Nr	Interaction	Elements
5	Vote (DF)	SiVES-S (Proc) and SiVES-C (Proc)

Threat: 14. Data Flow Sniffing			
Category: Information Disclosure			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
Data flowing across Vote may be sniffed by an attacker. Depending on what type of data an attacker can read, it may be used to attack other parts of the system or simply be a disclosure of information leading to compliance violations. Consider encrypting the data flow.	Data carried over unencrypted connections or use weak encryption algorithms	All connections must be strongly encrypted	

Threat: 15. Potential Process Crash or Stop for SiVES-S			
Category: Denial Of Service			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
SiVES-S crashes, halts, stops or runs slowly; in all cases violating an availability metric.	Inadequate or insufficient resources allow denial of service	The system must have means to avoid DoS attack, like redundancy.	
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them	

Identify Scenarios
Identify a possible 3-tuple (causal factor) from STRIDE

Nr	Interaction	Elements
5	Vote (DF)	SiVES-S (Proc) and SiVES-C (Proc)

Threat: 16. Data Flow Generic Is Potentially Interrupted			
Category: Denial Of Service			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
An external agent interrupts data flowing across a trust boundary in either direction.	Inadequate or insufficient resources allow denial of service	The system must have means to avoid DoS attack, like redundancy.	
	Physical access to system installation for DoS actions	Protect physical installation	

Threat: 17. Elevation Using Impersonation			
Category: Elevation Of Privilege			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
SiVES-S may be able to impersonate the context of SiVES-C in order to gain additional privilege.	Incorrect or insecure configuration	System configuration must be revised and hardened	
	Lack of training (competence) of system administrators, led to incorrect or insecure configurations	Administrators must be trained and have knowledge recycled regularly	
	There is no user authenation on SiVES-S from SiVES-C	The system shall provide user authentication	
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them	

Identify Scenarios
Identify a possible 3-tuple (causal factor) from STRIDE

Nr	Interaction	Elements
5	Vote (DF)	SiVES-S (Proc) and SiVES-C (Proc)

Threat: 18. SiVES-S May be Subject to Elevation of Privilege Using Remote Code Execution			
Category: Elevation Of Privilege			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
SiVES-C may be able to remotely execute code for SiVES-S.	There is no user authenation on SiVES-S from SiVES-C	The system shall provide user authentication	
	Inputs are not being validated	The input shall be validated	
	Data injection modifies system behavior	The system shall have the latest update of antimalware and shall remove the malware	
	Software not tested sufficiently before it goes into production	The application code must be thoroughly tested with the best methodologies before going into production	
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them	

Identify Scenarios
Identify a possible 3-tuple (causal factor) from STRIDE

Nr	Interaction	Elements
5	Vote (DF)	SiVES-S (Proc) and SiVES-C (Proc)

Threat: 19. Elevation by Changing the Execution Flow in SiVES-S			
Category: Elevation Of Privilege			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
An attacker may pass data into SiVES-S in order to change the flow of program execution within SiVES-S to the attacker's choosing.	Incorrect or insecure configuration	System configuration must be revised and hardened	
	Lack of training (competence) of system administrators, led to incorrect or insecure configurations	Administrators must be trained and have knowledge recycled regularly	
	Inputs are not being validated	The input shall be validated	
	Data injection modifies system behavior	The system shall have the latest update of antimalware and shall remove the malware	
	Software not tested sufficiently before it goes into production	The application code must be thoroughly tested with the best methodologies before going into production	
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them	

Identify Scenarios
Identify a possible 3-tuple (causal factor) from STRIDE

Nr	Interaction	Elements
5	Vote (DF)	SiVES-S (Proc) and SiVES-C (Proc)

Threat: 20. Cross Site Request Forgery			
Category: Elevation Of Privilege			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
Cross-site request forgery (CSRF or XSRF) is a type of attack in which an attacker forces a user's browser to make a forged request to a vulnerable site by exploiting an existing trust relationship between the browser and the vulnerable web site. In a simple scenario, a user is logged in to web site A using a cookie as a credential. The other browses to web site B. Web site B returns a page with a hidden form that posts to web site A. Since the browser will carry the user's cookie to web site A, web site B now can take any action on web site A, for example, adding an admin to an account. The attack can be used to exploit any requests that the browser automatically authenticates, e.g. by session cookie, integrated authentication, IP whitelisting, ... The attack can be carried out in many ways such as by luring the victim to a site under control of the attacker, getting the user to click a link in a phishing email, or hacking a reputable web site that the victim will visit. The issue can only be resolved on the server side by requiring that all authenticated state-changing requests include an additional piece of secret payload (canary or CSRF token) which is known only to the legitimate web site and the browser and which is protected in transit through SSL/TLS. See the Forgery Protection property on the flow stencil for a list of mitigations.	Incorrect or insecure configuration	System configuration must be revised and hardened	
	Lack of training (competence) of system administrators, led to incorrect or insecure configurations	Administrators must be trained and have knowledge recycled regularly	
	There is no user authenation on SiVES-S from SiVES-C	The system shall provide user authentication	
	Data carried over unencrypted connections or use weak encryption algorithms	All connections must be strongly encrypted	
	Software not tested sufficiently before it goes into production	The application code must be thoroughly tested with the best methodologies before going into production	
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them	

Identify Scenarios
Identify a possible 3-tuple (causal factor) from STRIDE

Nr	Interaction	Elements
6	Commands from VMS to Verification Machine (DF)	Verification Machine (Proc) and VMS (Proc)

Threat: 21. Spoofing the SiVES-C External Entity			
Category: Spoofing			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
VMS may be spoofed by an attacker and this may lead to unauthorized access to Verification Machine. Consider using a standard authentication mechanism to identify the external entity.	There is no user authenation on SiVES-S from SiVES-C	The system shall provide user authentication	
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them	

Threat: 22. Elevation Using Impersonation			
Category: Elevation Of Privilege			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
Verification Machine may be able to impersonate the context of VMS in order to gain additional privilege.	Incorrect or insecure configuration	System configuration must be revised and hardened	
	Lack of training (competence) of system administrators, led to incorrect or insecure configurations	Administrators must be trained and have knowledge recycled regularly	
	There is no user authenation on SiVES-S from SiVES-C	The system shall provide user authentication	
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them	

Identify Scenarios
Identify a possible 3-tuple (causal factor) from STRIDE

Nr	Interaction	Elements
7	Feedbacks from SiVES Servers to SiVES-S (DF)	SiVES-S (Proc) and SiVES Servers (Proc)

Threat: 23. Cross Site Scripting			
Category: Tampering			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
The server 'SiVES-S' could be a subject to a cross-site scripting attack because it does not sanitize untrusted input.	Inputs are not being validated	The input shall be validated	
	Data injection modifies system behavior	The system shall have the latest update of antimalware and shall remove the malware	

Threat: 24. Elevation Using Impersonation			
Category: Elevation Of Privilege			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
SiVES-S may be able to impersonate the context of SiVES Servers in order to gain additional privilege.	Incorrect or insecure configuration	System configuration must be revised and hardened	
	Lack of training (competence) of system administrators, led to incorrect or insecure configurations	Administrators must be trained and have knowledge recycled regularly	
	There is no user authenation on SiVES-S from SiVES-C	The system shall provide user authentication	
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them	

Identify Scenarios
Identify a possible 3-tuple (causal factor) from STRIDE

Nr	Interaction	Elements
8	Feedbacks from Virtual Stores to STI (DF)	STI (EE) and Virtual Stores (EE)

Threat: 25. External Entity STI Potentially Denies Receiving Data			
Category: Repudiation			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
STI claims that it did not receive data from a process on the other side of the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.	Inadequate or inexistent service control and logs	Provide logs and auditing to ensure non-repudiation	
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them	

Threat: 26. Data Flow Generic Is Potentially Interrupted			
Category: Denial Of Service			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
An external agent interrupts data flowing across a trust boundary in either direction.	Inadequate or insufficient resources allow denial of service	The system must have means to avoid DoS attack, like redundancy.	
	Physical access to system installation for DoS actions	Protect physical installation	

Identify Scenarios
Identify a possible 3-tuple (causal factor) from STRIDE

Nr	Interaction	Elements
9	Feedbacks/Data from SiVES-S DB to SiVES-S (DF)	SiVES-S DB (DS) and SiVES-S (Proc)

Threat: 27. Spoofing of Destination Data Store SQL Database			
Category: Spoofing			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
SiVES-S DB may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of SiVES-S DB. Consider using a standard authentication mechanism to identify the destination data store.	There is no user authenation on SiVES-S from SiVES-C	The system shall provide user authentication	
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them	

Threat: 28. Potential SQL Injection Vulnerability for SQL Database			
Category: Tampering			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
SQL injection is an attack in which malicious code is inserted into strings that are later passed to an instance of SQL Server for parsing and execution. Any procedure that constructs SQL statements should be reviewed for injection vulnerabilities because SQL Server will execute all syntactically valid queries that it receives. Even parameterized data can be manipulated by a skilled and determined attacker.	Inputs are not being validated	The input shall be validated	
	Data injection modifies system behavior	The system shall have the latest update of antimalware and shall remove the malware	

Identify Scenarios
Identify a possible 3-tuple (causal factor) from STRIDE

Nr	Interaction	Elements
9	Feedbacks/Data from SiVES-S DB to SiVES-S (DF)	SiVES-S DB (DS) and SiVES-S (Proc)

Threat: 29. Potential Excessive Resource Consumption for SiVES-S or SQL Database			
Category: Repudiation			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
Does SiVES-S or SiVES-S DB take explicit steps to control resource consumption? Resource consumption attacks can be hard to deal with, and there are times that it makes sense to let the OS do the job. Be careful that your resource requests don't deadlock, and that they do timeout.	Incorrect or insecure configuration	System configuration must be revised and hardened	
	Lack of training (competence) of system administrators, led to incorrect or insecure configurations	Administrators must be trained and have knowledge recycled regularly	
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them	

Identify Scenarios
Identify a possible 3-tuple (causal factor) from STRIDE

Nr	Interaction	Elements
9	Feedbacks/Data from SiVES-S DB to SiVES-S (DF)	SiVES-S DB (DS) and SiVES-S (Proc)

Threat: 30. Weak Credential Storage			
Category: Information Disclosure			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
Credentials held at the server are often disclosed or tampered with and credentials stored on the client are often stolen. For server side, consider storing a salted hash of the credentials instead of storing the credentials themselves. If this is not possible due to business requirements, be sure to encrypt the credentials before storage, using an SDL-approved mechanism. For client side, if storing credentials is required, encrypt them and protect the data store in which they're stored	Incorrect or insecure configuration	System configuration must be revised and hardened	
	Lack of training (competence) of system administrators, led to incorrect or insecure configurations	Administrators must be trained and have knowledge recycled regularly	
	Credentials are not hashed	Credentials must be stored considering salted hash	
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them	

Identify Scenarios
Identify a possible 3-tuple (causal factor) from STRIDE

Nr	Interaction	Elements
10	Insert/Select Data (from SiVES-S) on SiVES-S DB (DF)	SiVES-S DB (DS) and SiVES-S (Proc)

Threat: 31. Spoofing of Source Data Store SQL Database			
Category: Spoofing			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
SiVES-S DB may be spoofed by an attacker and this may lead to incorrect data delivered to SiVES-S. Consider using a standard authentication mechanism to identify the source data store.	There is no user authenation on SiVES-S from SiVES-C	The system shall provide user authentication	
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them	

Threat: 32. Cross Site Scripting			
Category: Tampering			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
The server 'SiVES-S' could be a subject to a cross-site scripting attack because it does not sanitize untrusted input.	Inputs are not being validated	The input shall be validated	
	Data injection modifies system behavior	The system shall have the latest update of antimalware and shall remove the malware	

Identify Scenarios
Identify a possible 3-tuple (causal factor) from STRIDE

Nr	Interaction	Elements
10	Insert/Select Data (from SiVES-S) on SiVES-S DB (DF)	SiVES-S DB (DS) and SiVES-S (Proc)

Threat: 33. Persistent Cross Site Scripting			
Category: Tampering			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
The server 'SiVES-S' could be a subject to a persistent cross-site scripting attack because it does not sanitize data store 'SiVES-S DB' inputs and output.	Inputs are not being validated	The input shall be validated	
	Data injection modifies system behavior	The system shall have the latest update of antimalware and shall remove the malware	

Threat: 34. Weak Access Control for a Resource			
Category: Information Disclosure			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
Improper data protection of SiVES-S DB can allow an attacker to read information not intended for disclosure. Review authorization settings.	Access permissions to SiVES-S DB is configured incorrectly	It must protect disclosure information by allowing access data only by predefined profiles.	
	Lack of training (competence) of system administrators, led to incorrect or insecure configurations	Administrators must be trained and have knowledge recycled regularly	
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them	

Identify Scenarios
Identify a possible 3-tuple (causal factor) from STRIDE

Nr	Interaction	Elements
11	Install or Update SiVES-C (DF)	Voter (EE) and Smartphone (Proc)

Threat: 35. Elevation Using Impersonation			
Category: Elevation Of Privilege			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
Smartphone may be able to impersonate the context of Voter in order to gain additional privilege.	Not applicable		

Threat: 36. Spoofing the Voter External Entity			
Category: Spoofing			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
Voter may be spoofed by an attacker and this may lead to unauthorized access to Smartphone. Consider using a standard authentication mechanism to identify the external entity.	Physical access to smartphone by attacker may permit improper access to all smartphone resources	Voter must be aware that he/she must have access to his/her smartphone by password and/or biometrics	
	Physical access to the smartphone by the attacker may allow malware installation	The voter must be aware that he must keep the smartphone to himself	

Identify Scenarios
Identify a possible 3-tuple (causal factor) from STRIDE

Nr	Interaction	Elements
12	Send IP Packets from SiVES Servers to Smartphone (DF)	SiVES Servers (Proc) and Smartphone (Proc)

Threat: 37. Elevation Using Impersonation			
Category: Elevation Of Privilege			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
Smartphone may be able to impersonate the context of SiVES Servers in order to gain additional privilege.	Incorrect or insecure configuration	System configuration must be revised and hardened	
	Lack of training (competence) of system administrators, led to incorrect or insecure configurations	Administrators must be trained and have knowledge recycled regularly	
	There is no user authenation on SiVES-S from SiVES-C	The system shall provide user authentication	
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them	

Threat: 38. Spoofing the SiVES Servers Process			
Category: Spoofing			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
SiVES Servers may be spoofed by an attacker and this may lead to unauthorized access to Smartphone. Consider using a standard authentication mechanism to identify the source process.	There is no user authenation on SiVES-S from SiVES-C	The system shall provide user authentication	
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them	

Identify Scenarios
Identify a possible 3-tuple (causal factor) from STRIDE

Nr	Interaction	Elements
12	Send IP Packets from SiVES Servers to Smartphone (DF)	SiVES Servers (Proc) and Smartphone (Proc)

Threat: 39. Spoofing the Smartphone Process			
Category: Spoofing			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
Smartphone may be spoofed by an attacker and this may lead to information disclosure by SiVES Servers. Consider using a standard authentication mechanism to identify the destination process.	There is no user authenation on SiVES-S from SiVES-C	The system shall provide user authentication	
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them	

Threat: 40. Potential Data Repudiation by Smartphone			
Category: Repudiation			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
Smartphone claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.	Inadequate or inexistent service control and logs	Provide logs and auditing to ensure non-repudiation	
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them	

Identify Scenarios
Identify a possible 3-tuple (causal factor) from STRIDE

Nr	Interaction	Elements
12	Send IP Packets from SiVES Servers to Smartphone (DF)	SiVES Servers (Proc) and Smartphone (Proc)

Threat: 41. Potential Process Crash or Stop for Smartphone			
Category: Denial Of Service			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
Smartphone crashes, halts, stops or runs slowly; in all cases violating an availability metric.	Inadequate or insufficient resources allow denial of service	The system must have means to avoid DoS attack, like redundancy.	
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them	

Threat: 42. Data Flow Send IP Packets from SiVES Servers to Smartphone Is Potentially Interrupted			
Category: Denial Of Service			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
An external agent interrupts data flowing across a trust boundary in either direction.	Inadequate or insufficient resources allow denial of service	The system must have means to avoid DoS attack, like redundancy.	
	Physical access to system installation for DoS actions	Protect physical installation	

Identify Scenarios
Identify a possible 3-tuple (causal factor) from STRIDE

Nr	Interaction	Elements
12	Send IP Packets from SiVES Servers to Smartphone (DF)	SiVES Servers (Proc) and Smartphone (Proc)

Threat: 43. Smartphone May be Subject to Elevation of Privilege Using Remote Code Execution			
Category: Elevation Of Privilege			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
SiVES Servers may be able to remotely execute code for Smartphone.	Incorrect or insecure configuration	System configuration must be revised and hardened	
	Lack of training (competence) of system administrators, led to incorrect or insecure configurations	Administrators must be trained and have knowledge recycled regularly	
	There is no user authenation on SiVES-S from SiVES-C	The system shall provide user authentication	
	Inputs are not being validated	The input shall be validated	
	Data injection modifies system behavior	The system shall have the latest update of antimalware and shall remove the malware	
	Software not tested sufficiently before it goes into production	The application code must be thoroughly tested with the best methodologies before going into production	
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them	

Identify Scenarios
Identify a possible 3-tuple (causal factor) from STRIDE

Nr	Interaction	Elements
12	Send IP Packets from SiVES Servers to Smartphone (DF)	SiVES Servers (Proc) and Smartphone (Proc)

Threat: 44. Elevation by Changing the Execution Flow in Smartphone			
Category: Elevation Of Privilege			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
An attacker may pass data into Smartphone in order to change the flow of program execution within Smartphone to the attacker's choosing.	Inputs are not being validated	The input shall be validated	
	Data injection modifies system behavior	The system shall have the latest update of antimalware and shall remove the malware	
	Data injection modifies system behavior	The system shall have the latest update of antimalware and shall remove the malware	
	Software not tested sufficiently before it goes into production	The application code must be thoroughly tested with the best methodologies before going into production	
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them	

Identify Scenarios
Identify a possible 3-tuple (causal factor) from STRIDE

Nr	Interaction	Elements
12	Send IP Packets from SiVES Servers to Smartphone (DF)	SiVES Servers (Proc) and Smartphone (Proc)

Threat: 45. Potential Lack of Input Validation for Smartphone			
Category: Tampering			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
Data flowing across Send IP Packets from SiVES Servers to Smartphone may be tampered with by an attacker. This may lead to a denial of service attack against Smartphone or an elevation of privilege attack against Smartphone or an information disclosure by Smartphone. Failure to verify that input is as expected is a root cause of a very large number of exploitable issues. Consider all paths and the way they handle data. Verify that all input is verified for correctness using an approved list input validation approach.	Inputs are not being validated	The input shall be validated	
	Data injection modifies system behavior	The system shall have the latest update of antimalware and shall remove the malware	

Identify Scenarios
Identify a possible 3-tuple (causal factor) from STRIDE

Nr	Interaction	Elements
12	Send IP Packets from SiVES Servers to Smartphone (DF)	SiVES Servers (Proc) and Smartphone (Proc)

Threat: 46. Data Flow Sniffing			
Category: Information Disclosure			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
Data flowing across Send IP Packets from SiVES Servers to Smartphone may be sniffed by an attacker. Depending on what type of data an attacker can read, it may be used to attack other parts of the system or simply be a disclosure of information leading to compliance violations. Consider encrypting the data flow.	There is no user authenation on SiVES-S from SiVES-C	The system shall provide user authentication	
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them	

Identify Scenarios
Identify a possible 3-tuple (causal factor) from STRIDE

Nr	Interaction	Elements
13	Send IP Packets from Smartphone to SiVES Servers (DF)	SiVES Servers (Proc) and Smartphone (Proc)

Threat: 47. Elevation Using Impersonation			
Category: Elevation Of Privilege			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
SiVES Servers may be able to impersonate the context of Smartphone in order to gain additional privilege.	Incorrect or insecure configuration	System configuration must be revised and hardened	
	Lack of training (competence) of system administrators, led to incorrect or insecure configurations	Administrators must be trained and have knowledge recycled regularly	
	There is no user authenation on SiVES-S from SiVES-C	The system shall provide user authentication	
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them	

Threat: 48. Spoofing the Smartphone Process			
Category: Spoofing			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
Smartphone may be spoofed by an attacker and this may lead to unauthorized access to SiVES Servers. Consider using a standard authentication mechanism to identify the source process.	There is no user authenation on SiVES-S from SiVES-C	The system shall provide user authentication	
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them	

Identify Scenarios
Identify a possible 3-tuple (causal factor) from STRIDE

Nr	Interaction	Elements
13	Send IP Packets from Smartphone to SiVES Servers (DF)	SiVES Servers (Proc) and Smartphone (Proc)

Threat: 49. Spoofing the SiVES Servers Process			
Category: Spoofing			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
SiVES Servers may be spoofed by an attacker and this may lead to information disclosure by Smartphone. Consider using a standard authentication mechanism to identify the destination process.	There is no user authenation on SiVES-S from SiVES-C	The system shall provide user authentication	
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them	

Threat: 50. Potential Data Repudiation by SiVES Servers			
Category: Repudiation			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
SiVES Servers claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.	Inadequate or inexistent service control and logs	Provide logs and auditing to ensure non-repudiation	
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them	

Identify Scenarios
Identify a possible 3-tuple (causal factor) from STRIDE

Nr	Interaction	Elements
13	Send IP Packets from Smartphone to SiVES Servers (DF)	SiVES Servers (Proc) and Smartphone (Proc)

Threat: 51. Potential Process Crash or Stop for SiVES Servers			
Category: Denial Of Service			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
SiVES Servers crashes, halts, stops or runs slowly; in all cases violating an availability metric.	Inadequate or insufficient resources allow denial of service	The system must have means to avoid DoS attack, like redundancy.	
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them	

Threat: 52. Data Flow Send IP Packets from Smartphone to SiVES Servers Is Potentially Interrupted			
Category: Denial Of Service			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
An external agent interrupts data flowing across a trust boundary in either direction.	Inadequate or insufficient resources allow denial of service	The system must have means to avoid DoS attack, like redundancy.	
	Physical access to system installation for DoS actions	Protect physical installation	

Identify Scenarios
Identify a possible 3-tuple (causal factor) from STRIDE

Nr	Interaction	Elements
13	Send IP Packets from Smartphone to SiVES Servers (DF)	SiVES Servers (Proc) and Smartphone (Proc)

Threat: 53. SiVES Servers May be Subject to Elevation of Privilege Using Remote Code Execution			
Category: Elevation Of Privilege			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
Smartphone may be able to remotely execute code for SiVES Servers.	Incorrect or insecure configuration	System configuration must be revised and hardened	
	Lack of training (competence) of system administrators, led to incorrect or insecure configurations	Administrators must be trained and have knowledge recycled regularly	
	There is no user authenation on SiVES-S from SiVES-C	The system shall provide user authentication	
	Inputs are not being validated	The input shall be validated	
	Data injection modifies system behavior	The system shall have the latest update of antimalware and shall remove the malware	
	Software not tested sufficiently before it goes into production	The application code must be thoroughly tested with the best methodologies before going into production	
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them	

Identify Scenarios
Identify a possible 3-tuple (causal factor) from STRIDE

Nr	Interaction	Elements
13	Send IP Packets from Smartphone to SiVES Servers (DF)	SiVES Servers (Proc) and Smartphone (Proc)

Threat: 54. Elevation by Changing the Execution Flow in SiVES Servers			
Category: Elevation Of Privilege			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
An attacker may pass data into SiVES Servers in order to change the flow of program execution within SiVES Servers to the attacker's choosing.	Inputs are not being validated	The input shall be validated	
	Data injection modifies system behavior	The system shall have the latest update of antimalware and shall remove the malware	
	Data injection modifies system behavior	The system shall have the latest update of antimalware and shall remove the malware	
	Software not tested sufficiently before it goes into production	The application code must be thoroughly tested with the best methodologies before going into production	
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them	

Identify Scenarios
Identify a possible 3-tuple (causal factor) from STRIDE

Nr	Interaction	Elements
13	Send IP Packets from Smartphone to SiVES Servers (DF)	SiVES Servers (Proc) and Smartphone (Proc)

Threat: 55. Potential Lack of Input Validation for SiVES Servers			
Category: Tampering			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
Data flowing across Send IP Packets from Smartphone to SiVES Servers may be tampered with by an attacker. This may lead to a denial of service attack against SiVES Servers or an elevation of privilege attack against SiVES Servers or an information disclosure by SiVES Servers. Failure to verify that input is as expected is a root cause of a very large number of exploitable issues. Consider all paths and the way they handle data. Verify that all input is verified for correctness using an approved list input validation approach.	Inputs are not being validated	The input shall be validated	
	Data injection modifies system behavior	The system shall have the latest update of antimalware and shall remove the malware	

Identify Scenarios
Identify a possible 3-tuple (causal factor) from STRIDE

Nr	Interaction	Elements
13	Send IP Packets from Smartphone to SiVES Servers (DF)	SiVES Servers (Proc) and Smartphone (Proc)

Threat: 56. Data Flow Sniffing			
Category: Information Disclosure			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
Data flowing across Send IP Packets from Smartphone to SiVES Servers may be sniffed by an attacker. Depending on what type of data an attacker can read, it may be used to attack other parts of the system or simply be a disclosure of information leading to compliance violations. Consider encrypting the data flow	There is no user authenation on SiVES-S from SiVES-C	The system shall provide user authentication	
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them	

Identify Scenarios
Identify a possible 3-tuple (causal factor) from STRIDE

Nr	Interaction	Elements
14	Smartphone Request App or Update to Virtual Stores (DF)	Virtual Stores (Proc) and Smartphone (Proc)

Threat: 57. Data Flow Generic Is Potentially Interrupted			
Category: Denial Of Service			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
An external agent interrupts data flowing across a trust boundary in either direction.	Inadequate or insufficient resources allow denial of service	The system must have means to avoid DoS attack, like redundancy.	
	Physical access to system installation for DoS actions	Protect physical installation	

Threat: 58. External Entity Virtual Stores Potentially Denies Receiving Data			
Category: Denial Of Service			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
Virtual Stores claims that it did not receive data from a process on the other side of the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.	Inadequate or inexistent service control and logs	Provide logs and auditing to ensure non-repudiation	
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them	

Identify Scenarios
Identify a possible 3-tuple (causal factor) from STRIDE

Nr	Interaction	Elements
14	Smartphone Request App or Update to Virtual Stores (DF)	Virtual Stores (Proc) and Smartphone (Proc)

Threat: 59. Spoofing of the Virtual Stores External Destination Entity			
Category: Denial Of Service			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
Virtual Stores may be spoofed by an attacker and this may lead to data being sent to the attacker's target instead of Virtual Stores. Consider using a standard authentication mechanism to identify the external entity.	There is no user authenation on SiVES-S from SiVES-C	The system shall provide user authentication	
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them	

Identify Scenarios
Identify a possible 3-tuple (causal factor) from STRIDE

Nr	Interaction	Elements
15	STI Monitoring SiVES-S (DF)	STI (EE) and SiVES-S (Proc)

Threat: 60. Spoofing the STI External Entity			
Category: Spoofing			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
STI may be spoofed by an attacker and this may lead to unauthorized access to SiVES-S. Consider using a standard authentication mechanism to identify the external entity.	There is no user authenation on SiVES-S from SiVES-C	The system shall provide user authentication	
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them	

Threat: 61. Cross Site Scripting			
Category: Tampering			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
The server 'SiVES-S' could be a subject to a cross-site scripting attack because it does not sanitize untrusted input.	Inputs are not being validated	The input shall be validated	
	Data injection modifies system behavior	The system shall have the latest update of antimalware and shall remove the malware	

Identify Scenarios
Identify a possible 3-tuple (causal factor) from STRIDE

Nr	Interaction	Elements
15	STI Monitoring SiVES-S (DF)	STI (EE) and SiVES-S (Proc)

Threat: 62. Elevation Using Impersonation			
Category: Elevation Of Privilege			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
SiVES-S may be able to impersonate the context of STI in order to gain additional privilege.	Incorrect or insecure configuration	System configuration must be revised and hardened	
	Lack of training (competence) of system administrators, led to incorrect or insecure configurations	Administrators must be trained and have knowledge recycled regularly	
	There is no user authenation on SiVES-S from SiVES-C	The system shall provide user authentication	
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them	

Identify Scenarios
Identify a possible 3-tuple (causal factor) from STRIDE

Nr	Interaction	Elements
16	Virtual Stores send App or Information about new version to Smartphone (DF)	Virtual Stores (Proc) and Smartphone (Proc)

Threat: 63. Elevation by Changing the Execution Flow in Smartphone			
Category: Elevation Of Privilege			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
An attacker may pass data into Smartphone in order to change the flow of program execution within Smartphone to the attacker's choosing.	Incorrect or insecure configuration	System configuration must be revised and hardened	
	Lack of training (competence) of system administrators, led to incorrect or insecure configurations	Administrators must be trained and have knowledge recycled regularly	
	Inputs are not being validated	The input shall be validated	
	Data injection modifies system behavior	The system shall have the latest update of antimalware and shall remove the malware	
	Software not tested sufficiently before it goes into production	The application code must be thoroughly tested with the best methodologies before going into production	
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them	

Identify Scenarios
Identify a possible 3-tuple (causal factor) from STRIDE

Nr	Interaction	Elements
16	Virtual Stores send App or Information about new version to Smartphone (DF)	Virtual Stores (Proc) and Smartphone (Proc)

Threat: 64. Smartphone May be Subject to Elevation of Privilege Using Remote Code Execution			
Category: Elevation Of Privilege			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
Virtual Stores may be able to remotely execute code for Smartphone.	There is no user authenation on SiVES-S from SiVES-C	The system shall provide user authentication	
	Inputs are not being validated	The input shall be validated	
	Data injection modifies system behavior	The system shall have the latest update of antimalware and shall remove the malware	
	Software not tested sufficiently before it goes into production	The application code must be thoroughly tested with the best methodologies before going into production	
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them	

Identify Scenarios
Identify a possible 3-tuple (causal factor) from STRIDE

Nr	Interaction	Elements
16	Virtual Stores send App or Information about new version to Smartphone (DF)	Virtual Stores (Proc) and Smartphone (Proc)

Threat: 65. Elevation Using Impersonation			
Category: Elevation Of Privilege			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
Smartphone may be able to impersonate the context of Virtual Stores in order to gain additional privilege.	Incorrect or insecure configuration	System configuration must be revised and hardened	
	Lack of training (competence) of system administrators, led to incorrect or insecure configurations	Administrators must be trained and have knowledge recycled regularly	
	There is no user authenation on SiVES-S from SiVES-C	The system shall provide user authentication	
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them	

Identify Scenarios
Identify a possible 3-tuple (causal factor) from STRIDE

Nr	Interaction	Elements
16	Virtual Stores send App or Information about new version to Smartphone (DF)	Virtual Stores (Proc) and Smartphone (Proc)

Threat: 66. Data Flow Generic Is Potentially Interrupted			
Category: Denial Of Service			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
An external agent interrupts data flowing across a trust boundary in either direction.	Inadequate or insufficient resources allow denial of service	The system must have means to avoid DoS attack, like redundancy.	
	Physical access to system installation for DoS actions	Protect physical installation	

Threat: 67. Potential Process Crash or Stop for Smartphone			
Category: Denial Of Service			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
Smartphone crashes, halts, stops or runs slowly; in all cases violating an availability metric.	Inadequate or insufficient resources allow denial of service	The system must have means to avoid DoS attack, like redundancy.	
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them	

Identify Scenarios
Identify a possible 3-tuple (causal factor) from STRIDE

Nr	Interaction	Elements
16	Virtual Stores send App or Information about new version to Smartphone (DF)	Virtual Stores (Proc) and Smartphone (Proc)

Threat: 68. Data Flow Sniffing			
Category: Information Disclosure			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
Data flowing across Virtual Stores send App or Information about new version to Smartphone may be sniffed by an attacker. Depending on what type of data an attacker can read, it may be used to attack other parts of the system or simply be a disclosure of information leading to compliance violations. Consider encrypting the data flow.	Data carried over unencrypted connections or use weak encryption algorithms	All connections must be strongly encrypted	

Threat: 69. Potential Data Repudiation by Smartphone			
Category: Repudiation			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
Smartphone claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.	Inadequate or inexistent service control and logs	Provide logs and auditing to ensure non-repudiation	
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them	

Identify Scenarios
Identify a possible 3-tuple (causal factor) from STRIDE

Nr	Interaction	Elements
16	Virtual Stores send App or Information about new version to Smartphone (DF)	Virtual Stores (Proc) and Smartphone (Proc)

Threat: 70. Potential Lack of Input Validation for Smartphone			
Category: Tampering			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
Data flowing across Virtual Stores send App or Information about new version to Smartphone may be tampered with by an attacker. This may lead to a denial of service attack against Smartphone or an elevation of privilege attack against Smartphone or an information disclosure by Smartphone. Failure to verify that input is as expected is a root cause of a very large number of exploitable issues. Consider all paths and the way they handle data. Verify that all input is verified for correctness using an approved list input validation approach.	Inputs are not being validated	The input shall be validated	
	Data injection modifies system behavior	The system shall have the latest update of antimalware and shall remove the malware	

Identify Scenarios
Identify a possible 3-tuple (causal factor) from STRIDE

Nr	Interaction	Elements
16	Virtual Stores send App or Information about new version to Smartphone (DF)	Virtual Stores (Proc) and Smartphone (Proc)

Threat: 71. Spoofing the Virtual Stores External Entity			
Category: Spoofing			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
Virtual Stores may be spoofed by an attacker and this may lead to unauthorized access to Smartphone. Consider using a standard authentication mechanism to identify the external entity.	There is no user authenation on SiVES-S from SiVES-C	The system shall provide user authentication	
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them	

Threat: 72. Spoofing the Smartphone Process			
Category: Spoofing			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
Smartphone may be spoofed by an attacker and this may lead to information disclosure by Virtual Stores. Consider using a standard authentication mechanism to identify the destination process.	There is no user authenation on SiVES-S from SiVES-C	The system shall provide user authentication	
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them	

Identify Scenarios
Identify a possible 3-tuple (causal factor) from STRIDE

Nr	Interaction	Elements
17	Voter´s Level of Acceptance (DF)	TSE (EE) and Voter (EE)

Threat: 73. Authenticated Data Flow Compromised			
Category: Tampering			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
An attacker can read or modify data transmitted over an authenticated dataflow.	Incorrect or insecure configuration	System configuration must be revised and hardened	
	Lack of training (competence) of system administrators, led to incorrect or insecure configurations	Administrators must be trained and have knowledge recycled regularly	
	Data injection modifies system behavior	The system shall have the latest update of antimalware and shall remove the malware	
	Software not tested sufficiently before it goes into production	The application code must be thoroughly tested with the best methodologies before going into production	
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them	

Identify Scenarios
Identify a possible 3-tuple (causal factor) from STRIDE

Nr	Interaction	Elements
17	Voter´s Vote Request (DF)	VMS (Proc) and SiVES-S (Proc)

Threat: 74. Spoofing the SiVES-S Process			
Category: Spoofing			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
SiVES-S may be spoofed by an attacker and this may lead to information disclosure by VMS. Consider using a standard authentication mechanism to identify the destination process.	There is no user authenation on SiVES-S from SiVES-C	The system shall provide user authentication	
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them	

Threat: 75. Spoofing the VMS External Entity			
Category: Spoofing			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
VMS may be spoofed by an attacker and this may lead to unauthorized access to SiVES-S. Consider using a standard authentication mechanism to identify the external entity.	There is no user authenation on SiVES-S from SiVES-C	The system shall provide user authentication	
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them	

Identify Scenarios
Identify a possible 3-tuple (causal factor) from STRIDE

Nr	Interaction	Elements
17	Voter´s Vote Request (DF)	VMS (Proc) and SiVES-S (Proc)

Threat: 76. Potential Lack of Input Validation for SiVES-S			
Category: Tampering			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
Data flowing across Voter´s Vote Request may be tampered with by an attacker. This may lead to a denial of service attack against SiVES-S or an elevation of privilege attack against SiVES-S or an information disclosure by SiVES-S. Failure to verify that input is as expected is a root cause of a very large number of exploitable issues. Consider all paths and the way they handle data. Verify that all input is verified for correctness using an approved list input validation approach.	Inputs are not being validated	The input shall be validated	
	Data injection modifies system behavior	The system shall have the latest update of antimalware and shall remove the malware	

Identify Scenarios
Identify a possible 3-tuple (causal factor) from STRIDE

Nr	Interaction	Elements
17	Voter´s Vote Request (DF)	VMS (Proc) and SiVES-S (Proc)

Threat: 77. Cross Site Scripting			
Category: Tampering			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
The server 'SiVES-S' could be a subject to a cross-site scripting attack because it does not sanitize untrusted input.	Inputs are not being validated	The input shall be validated	
	Data injection modifies system behavior	The system shall have the latest update of antimalware and shall remove the malware	

Threat: 78. Potential Data Repudiation by SiVES-S			
Category: Repudiation			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
SiVES-S claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.	Inadequate or inexistent service control and logs	Provide logs and auditing to ensure non-repudiation	
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them	

Identify Scenarios
Identify a possible 3-tuple (causal factor) from STRIDE

Nr	Interaction	Elements
17	Voter´s Vote Request (DF)	VMS (Proc) and SiVES-S (Proc)

Threat: 79. Data Flow Sniffing			
Category: Spoofing			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
Data flowing across Voter´s Vote Request may be sniffed by an attacker. Depending on what type of data an attacker can read, it may be used to attack other parts of the system or simply be a disclosure of information leading to compliance violations. Consider encrypting the data flow.	Data carried over unencrypted connections or use weak encryption algorithms	All connections must be strongly encrypted	

Threat: 80. Potential Process Crash or Stop for SiVES-S			
Category: Denial Of Service			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
SiVES-S crashes, halts, stops or runs slowly; in all cases violating an availability metric	Inadequate or insufficient resources allow denial of service	The system must have means to avoid DoS attack, like redundancy.	
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them	

Identify Scenarios
Identify a possible 3-tuple (causal factor) from STRIDE

Nr	Interaction	Elements
17	Voter´s Vote Request (DF)	VMS (Proc) and SiVES-S (Proc)

Threat: 81. Data Flow Generic Is Potentially Interrupted			
Category: Denial Of Service			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
An external agent interrupts data flowing across a trust boundary in either direction.	Inadequate or insufficient resources allow denial of service	The system must have means to avoid DoS attack, like redundancy.	
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them	

Threat: 82. Elevation Using Impersonation			
Category: Elevation Of Privilege			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
SiVES-S may be able to impersonate the context of VMS in order to gain additional privilege	Incorrect or insecure configuration	System configuration must be revised and hardened	
	Lack of training (competence) of system administrators, led to incorrect or insecure configurations	Administrators must be trained and have knowledge recycled regularly	
	There is no user authenation on SiVES-S from SiVES-C	The system shall provide user authentication	
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them	

Identify Scenarios
Identify a possible 3-tuple (causal factor) from STRIDE

Nr	Interaction	Elements
17	Voter´s Vote Request (DF)	VMS (Proc) and SiVES-S (Proc)

Threat: 83. SiVES-S May be Subject to Elevation of Privilege Using Remote Code Execution			
Category: Elevation Of Privilege			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
VMS may be able to remotely execute code for SiVES-S.	There is no user authenation on SiVES-S from SiVES-C	The system shall provide user authentication	
	Inputs are not being validated	The input shall be validated	
	Data injection modifies system behavior	The system shall have the latest update of antimalware and shall remove the malware	
	Software not tested sufficiently before it goes into production	The application code must be thoroughly tested with the best methodologies before going into production	
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them	

Identify Scenarios
Identify a possible 3-tuple (causal factor) from STRIDE

Nr	Interaction	Elements
17	Voter´s Vote Request (DF)	VMS (Proc) and SiVES-S (Proc)

Threat: 84. Elevation by Changing the Execution Flow in SiVES-S			
Category: Elevation Of Privilege			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
An attacker may pass data into SiVES-S in order to change the flow of program execution within SiVES-S to the attacker's choosing.	Incorrect or insecure configuration	System configuration must be revised and hardened	
	Lack of training (competence) of system administrators, led to incorrect or insecure configurations	Administrators must be trained and have knowledge recycled regularly	
	Inputs are not being validated	The input shall be validated	
	Data injection modifies system behavior	The system shall have the latest update of antimalware and shall remove the malware	
	Software not tested sufficiently before it goes into production	The application code must be thoroughly tested with the best methodologies before going into production	
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them	

Identify Scenarios
Identify a possible 3-tuple (causal factor) from STRIDE

Nr	Interaction	Elements
17	Voter´s Vote Request (DF)	VMS (Proc) and SiVES-S (Proc)

Threat: 85. Cross Site Request Forgery			
Category: Elevation Of Privilege			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
Cross-site request forgery (CSRF or XSRF) is a type of attack in which an attacker forces a user's browser to make a forged request to a vulnerable site by exploiting an existing trust relationship between the browser and the vulnerable web site. In a simple scenario, a user is logged in to web site A using a cookie as a credential. The other browses to web site B. Web site B returns a page with a hidden form that posts to web site A. Since the browser will carry the user's cookie to web site A, web site B now can take any action on web site A, for example, adding an admin to an account. The attack can be used to exploit any requests that the browser automatically authenticates, e.g. by session cookie, integrated authentication, IP whitelisting, ... The attack can be carried out in many ways such as by luring the victim to a site under control of the attacker, getting the user to click a link in a phishing email, or hacking a reputable web site that the victim will visit. The issue can only be resolved on the server side by requiring that all authenticated state-changing requests include an additional piece of secret payload (canary or CSRF token) which is known only to the legitimate web site and the browser and which is protected in transit through SSL/TLS. See the Forgery Protection property on the flow stencil for a list of mitigations. Justification: It is necessary to harden system, use authentication and encrypted connections to avoid all these attacks.	Incorrect or insecure configuration	System configuration must be revised and hardened	
	Lack of training (competence) of system administrators, led to incorrect or insecure configurations	Administrators must be trained and have knowledge recycled regularly	
	There is no user authenation on SiVES-S from SiVES-C	The system shall provide user authentication	
	Data carried over unencrypted connections or use weak encryption algorithms	All connections must be strongly encrypted	
	Software not tested sufficiently before it goes into production	The application code must be thoroughly tested with the best methodologies before going into production	
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them	

Identify Scenarios
Identify a possible 3-tuple (causal factor) from STRIDE

Nr	Interaction	Elements
18	Voter´s Vote (DF)	VMS (Proc) and SiVES-S (Proc)

Threat: 86. Spoofing of the VMS External Destination Entity			
Category: Spoofing			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
VMS may be spoofed by an attacker and this may lead to data being sent to the attacker's target instead of VMS. Consider using a standard authentication mechanism to identify the external entity.	There is no user authenation on SiVES-S from SiVES-C	The system shall provide user authentication	
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them	

Threat: 87. External Entity VMS Potentially Denies Receiving Data			
Category: Repudiation			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
VMS claims that it did not receive data from a process on the other side of the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.	Inadequate or inexistent service control and logs	Provide logs and auditing to ensure non-repudiation	
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them	

Identify Scenarios
Identify a possible 3-tuple (causal factor) from STRIDE

Nr	Interaction	Elements
18	Voter´s Vote (DF)	VMS (Proc) and SiVES-S (Proc)

Threat: 88. Data Flow Generic Is Potentially Interrupted			
Category: Denial Of Service			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
An external agent interrupts data flowing across a trust boundary in either direction.	Inadequate or insufficient resources allow denial of service	The system must have means to avoid DoS attack, like redundancy.	
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them	

Identify Scenarios
Identify a possible 3-tuple (causal factor) from STRIDE

8. Analysis threats directly against each **isolated** element

Threats against: 89. TSE (EE)			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
The attacks against the TSE could not change the electronic voting system, because the TSE judges electoral conflicts, but does not create rules, nor does it implement them and any maliciously altered rules would be realized before being implemented.			

Threats against: 90. STI (EE)			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
Data exposed	Physical attack against the STI building for data theft	Protect STI building against undue access	
System Offline	Physical attack against the STI building and internet links to stop electronic voting service	Protect STI building against physical attacks and against links	
		Build datacenter backup to prevent physical attack to stop service	

Identify Scenarios
Identify a possible 3-tuple (causal factor) from STRIDE

8. Analysis threats directly against each **isolated** element

Threats against: 91. Electoral Office (EE)			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
The same physical threats against STI			

Threats against: 92. Virtual Stores (EE)			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
Fake Virtual Stores Host sends fake App to Smartphone	Compromised script of installation or update	The Virtual Stores security team must alert about fake hosts and prevent any compromise of its internal security	
	Fake Virtual Store Host	The manufacturer contract with the Virtual Stores must penalize the companies for such failures	
	Lack of voter awareness of minimum security precautions with your smartphone	The voter must be aware of the need for minimum security precautions with his smartphone that do not compromise his own vote	This causal factors affects security and privacy aspects

Identify Scenarios
Identify a possible 3-tuple (causal factor) from STRIDE

8. Analysis threats directly against each **isolated** element

Threats against: 93. Voter (EE)			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
Threats against the voter are related to coercion for the voter to vote for a candidate who offends the privacy of one or other specific voter. Despite this, this attack will not be considered, as it is very unlikely that it can be executed on a large scale, which could compromise the electronic voting system by the smartphone.			

Threats against: 94. Smartphone (EE)			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
Voter and his/her vote exposed on a large scale	Malware infects large amount of smartphones to change its functioning and to leak information from the electronic voting system through each smartphone	SiVES must check if smartphone has updated anti-malware and just so to allow voting	
Voters are prevented from voting	Malware in smartphones operating system leaks information		
At any stage of the voting procedure, large number of voters claims that his/her vote was modified or disclosed by system error	Malware infects large amount of smartphones to change voter´s vote		

Identify Scenarios
Identify a possible 3-tuple (causal factor) from STRIDE

8. Analysis threats directly against each **isolated** element

Threats against: 95. SiVES-C (Proc)			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
The same threats against Smartphone			

Threats against: 96. SiVES Servers (Proc)			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
The same threats against STI			

Threats against: 97. SiVES-S (Proc)			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
The same threats against Smartphone by malware and/or intrusion and SiVES must check if smartphone has updated anti-malware and just so to allow voting and it must be checked continuously by Pentest Team and if a intrusion occurs the damages must be limited by a Computer Emergency Response Team – CERT.			

Identify Scenarios
Identify a possible 3-tuple (causal factor) from STRIDE

8. Analysis threats directly against each **isolated** element

Threats against: 98. Verification Machine (Proc)			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
The same threats against Smartphone			

Threats against: 99. VMS (Proc)			
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**
The same threats against Smartphone			

Process to identify the security requirements - Overview

The process to identify the security requirements is:

- Execute steps 1, 2 and 3
- Execute activities 4.1 and 4.2 from STPA Step 4
- Map model elements and obtain the DFD (DIEFD) from CS (Task 4.3.1)
- Identify threats and vulnerabilities in DIEFD (STRIDE Analysis) (Task 4.3.2)
- Identify scenarios (Task 4.3.3)
- Consolidate Losses (Activity 4.4): for each HCA, verify which 3-tuple can be a causal factor. If it can be, generate a requirement (recommendation) with redundancy check (NEW and REP states)

Consolidate Losses

Control Action: Send the voter’s vote to SiVES-S (SiVES-C) (CA Nr 20)
Hazardous Control Action: SiVES-C not provide send the voter’s vote to SiVES-S when sives_s_authenticated_user is no and sives_s_available_status_ok is no (provided)
Group 1 (Right Side): hazardous control action provided or safe control action required but not provided (issued)

Consolidate Losses

NOTE 1: For simplicity of analysis and not to make this presentation very much extensive, we will only test one Hazardous Control Action for a single Control Action.

NOTE 2: After verifying that the scenario is applicable, you need to check the redundancies with Task 5 scenarios and set whether it is new (NEW) or repeated with STPA (REP1) or with STRIDE itself (REP2).

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)					
Hazardous Control Action: SiVES-C not provide send the voter's vote to SiVES-S when sives_s_authenticated_user is no and sives_s_available_status_ok is no (provided)					
Group 1 (Right Side): hazardous control action provided or safe control action required but not provided (issued)					
Interaction		**Elements**			
Commands from SiVES-C to Smartphone (DF)		SiVES-C (Proc) and Smartphone (Proc)			
Threat: 1. Spoofing the SiVES-C External Entity					
Category: Spoofing					
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**	**Pertinent?**	**New or repeated?**
SiVES-C may be spoofed by an attacker and this may lead to unauthorized access to Smartphone. Consider using a standard authentication mechanism to identify the external entity.	There is no user authenation on SiVES-S from SiVES-C	The system shall provide user authentication		Yes	NEW
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them		Yes	REP2

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)					
Hazardous Control Action: SiVES-C not provide send the voter's vote to SiVES-S when sives_s_authenticated_user is no and sives_s_available_status_ok is no (provided)					
Group 1 (Right Side): hazardous control action provided or safe control action required but not provided (issued)					
Interaction		**Elements**			
Commands from SiVES-C to Smartphone (DF)		SiVES-C (Proc) and Smartphone (Proc)			
Threat: 2. Elevation Using Impersonation					
Category: Elevation of Privilege					
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**	**Pertinent?**	**New or repeated?**
Smartphone may be able to impersonate the context of SiVES-C in order to gain additional privilege.	Incorrect or insecure configuration	System configuration must be revised and hardened		Yes	NEW
	Lack of training (competence) of system administrators, led to incorrect or insecure configurations	Administrators must be trained and have knowledge recycled regularly		Yes	NEW
	There is no user authenation on SiVES-S from SiVES-C	The system shall provide user authentication		Yes	REP2
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them		Yes	REP2

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)					
Hazardous Control Action: SiVES-C not provide send the voter's vote to SiVES-S when sives_s_authenticated_user is no and sives_s_available_status_ok is no (provided)					
Group 1 (Right Side): hazardous control action provided or safe control action required but not provided (issued)					
Interaction		**Elements**			
Commands from SiVES-S to SiVES Servers (DF)		SiVES-S (Proc) and SiVES Servers (Proc)			
Threat: 3. Elevation Using Impersonation					
Category: Elevation of Privilege					
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**	**Pertinent?**	**New or repeated?**
SiVES Servers may be able to impersonate the context of SiVES-S in order to gain additional privilege.	Incorrect or insecure configuration	System configuration must be revised and hardened		Yes	REP2
	Lack of training (competence) of system administrators, led to incorrect or insecure configurations	Administrators must be trained and have knowledge recycled regularly		Yes	REP2
	There is no user authenation on SiVES-S from SiVES-C	The system shall provide user authentication		Yes	REP2
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them		Yes	REP2

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)					
Hazardous Control Action: SiVES-C not provide send the voter's vote to SiVES-S when sives_s_authenticated_user is no and sives_s_available_status_ok is no (provided)					
Group 1 (Right Side): hazardous control action provided or safe control action required but not provided (issued)					
Interaction		**Elements**			
Commands from SiVES-S to SiVES Servers (DF)		SiVES-S (Proc) and SiVES Servers (Proc)			
Threat: 3. Elevation Using Impersonation					
Category: Elevation of Privilege					
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**	**Pertinent?**	**New or repeated?**
SiVES-C may be spoofed by an attacker and this may lead to information disclosure by SIVES-Sr using a standard authentication mechanism to identify the external entity.	There is no user authenation on SiVES-S from SiVES-C	The system shall provide user authentication		Yes	REP2
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them		Yes	REP2

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)					
Hazardous Control Action: SiVES-C not provide send the voter's vote to SiVES-S when sives_s_authenticated_user is no and sives_s_available_status_ok is no (provided)					
Group 1 (Right Side): hazardous control action provided or safe control action required but not provided (issued)					
Interaction		**Elements**			
Feedbacks from SiVES-S to SiVES-C (DF)		SiVES-C (Proc) and SiVES-S (Proc)			
Threat: 4. Spoofing of the SiVES-C External Destination Entity					
Category: Spoofing					
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**	**Pertinent?**	**New or repeated?**
SiVES-C may be spoofed by an attacker and this may lead to information disclosure by SIVES-S	There is no user authenation on SiVES-S from SiVES-C	System must provide user authentication		Yes	REP2
	No cliente to server authentication and vice versa	The system shall provide authentication for both directions		Yes	NEW
	Presence of software bugs	The software shall be continuously tested and maintained.		Yes	REP2

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)					
Hazardous Control Action: SiVES-C not provide send the voter's vote to SiVES-S when sives_s_authenticated_user is no and sives_s_available_status_ok is no (provided)					
Group 1 (Right Side): hazardous control action provided or safe control action required but not provided (issued)					
Interaction		**Elements**			
Feedbacks from SiVES-S to SiVES-C (DF)		SiVES-C (Proc) and SiVES-S (Proc)			
Threat: 5. External Entity SiVES-C Potentially Denies Receiving Data					
Category: Repudiation					
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**	**Pertinent?**	**New or repeated?**
SiVES-C claims that it did not receive data from a process on the other side of the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.	Inadequate or inexistent service control and logs	Provide logs and auditing to ensure non-repudiation		Yes	NEW
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them		Yes	REP2

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)					
Hazardous Control Action: SiVES-C not provide send the voter's vote to SiVES-S when sives_s_authenticated_user is no and sives_s_available_status_ok is no (provided)					
Group 1 (Right Side): hazardous control action provided or safe control action required but not provided (issued)					
Interaction		**Elements**			
Feedbacks from SiVES-S to SiVES-C (DF)		SiVES-C (Proc) and SiVES-S (Proc)			
Threat: 6. Data Flow Generic Is Potentially Interrupted					
Category: Denial Of Service					
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**	**Pertinent?**	**New or repeated?**
An external agent interrupts data flowing across a trust boundary in either direction.	Inadequate or insufficient resources allow denial of service	The system must have means to avoid DoS attack, like redundancy.		Yes	NEW
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them		Yes	REP2

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)					
Hazardous Control Action: SiVES-C not provide send the voter's vote to SiVES-S when sives_s_authenticated_user is no and sives_s_available_status_ok is no (provided)					
Group 1 (Right Side): hazardous control action provided or safe control action required but not provided (issued)					
Interaction		**Elements**			
Vote (DF)		SiVES-S (Proc) and SiVES-C (Proc)			
Threat: 9. Spoofing the SiVES-S Process					
Category: Spoofing					
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**	**Pertinent?**	**New or repeated?**
SiVES-S may be spoofed by an attacker and this may lead to information disclosure by SiVES-C. Consider using a standard authentication mechanism to identify the destination process.	There is no user authenation on SiVES-S from SiVES-C	The system shall provide user authentication		Yes	REP2
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them		Yes	REP2

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)					
Hazardous Control Action: SiVES-C not provide send the voter's vote to SiVES-S when sives_s_authenticated_user is no and sives_s_available_status_ok is no (provided)					
Group 1 (Right Side): hazardous control action provided or safe control action required but not provided (issued)					
Interaction		**Elements**			
Vote (DF)		SiVES-S (Proc) and SiVES-C (Proc)			
Threat: 10. Spoofing the SiVES-C External Entity					
Category: Spoofing					
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**	**Pertinent?**	**New or repeated?**
SiVES-C may be spoofed by an attacker and this may lead to unauthorized access to SiVES-S. Consider using a standard authentication mechanism to identify the external entity.	There is no user authenation on SiVES-S from SiVES-C	The system shall provide user authentication		Yes	REP2
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them		Yes	REP2

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)					
Hazardous Control Action: SiVES-C not provide send the voter's vote to SiVES-S when sives_s_authenticated_user is no and sives_s_available_status_ok is no (provided)					
Group 1 (Right Side): hazardous control action provided or safe control action required but not provided (issued)					
Interaction		**Elements**			
Vote (DF)		SiVES-S (Proc) and SiVES-C (Proc)			
Threat: 11. Potential Lack of Input Validation for SiVES-S					
Category: Tampering					
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**	**Pertinent?**	**New or repeated?**
Data flowing across Vote may be tampered with by an attacker. This may lead to a denial of service attack against SiVES-S or an elevation of privilege attack against SiVES-S or an information disclosure by SiVES-S.	SiVES-S inputs is not validated	The input shall be validated		No	---
	Connection failure between SiVES-C and SiVES-S	Since the connection is made using Internet, nothing can be made. We assume that TCP handles the failure		No	---
	Intentional Tampering of data by external agent	The system shall provide message integrity check mechanism		No	---
	SiVES-C output is not validated	The output shall be validated		No	---
	Incorrect or insecure SiVES-S configuration	The SiVES-S configuration shall be reviewed and hardened.		No	---
	Lack of knowledge of system administrators that leads to incorrect or insecure settings	The system administrators shall be regularly recycled		No	---
	Presence of software bugs in SiVES-S and/or SiVES-C	The software shall be continuously tested and maintained.		No	---

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)					
Hazardous Control Action: SiVES-C not provide send the voter's vote to SiVES-S when sives_s_authenticated_user is no and sives_s_available_status_ok is no (provided)					
Group 1 (Right Side): hazardous control action provided or safe control action required but not provided (issued)					
Interaction		**Elements**			
Vote (DF)		SiVES-S (Proc) and SiVES-C (Proc)			
Threat: 12. Cross Site Scripting					
Category: Tampering					
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**	**Pertinent?**	**New or repeated?**
The server 'SiVES-S' could be a subject to a cross-site scripting attack because it does not sanitize untrusted input.	Inputs are not being validated	The input shall be validated		Yes	REP2
	Data injection modifies system behavior	The system shall have the latest update of antimalware and shall remove the malware		Yes	NEW

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)					
Hazardous Control Action: SiVES-C not provide send the voter's vote to SiVES-S when sives_s_authenticated_user is no and sives_s_available_status_ok is no (provided)					
Group 1 (Right Side): hazardous control action provided or safe control action required but not provided (issued)					
Interaction	**Elements**				
Vote (DF)	SiVES-S (Proc) and SiVES-C (Proc)				
Threat: 13. Potential Data Repudiation by SiVES-S					
Category: Repudiation					
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**	**Pertinent?**	**New or repeated?**
SiVES-S claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.	Inadequate or inexistent service control and logs	Provide logs and auditing to ensure non-repudiation		Yes	REP2
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them		Yes	REP2

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)					
Hazardous Control Action: SiVES-C not provide send the voter's vote to SiVES-S when sives_s_authenticated_user is no and sives_s_available_status_ok is no (provided)					
Group 1 (Right Side): hazardous control action provided or safe control action required but not provided (issued)					
Interaction		**Elements**			
Vote (DF)		SiVES-S (Proc) and SiVES-C (Proc)			
Threat: 14. Data Flow Sniffing					
Category: Information Disclosure					
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**	**Pertinent?**	**New or repeated?**
Data flowing across Vote may be sniffed by an attacker. Depending on what type of data an attacker can read, it may be used to attack other parts of the system or simply be a disclosure of information leading to compliance violations. Consider encrypting the data flow.	Data carried over unencrypted connections or use weak encryption algorithms	All connections must be strongly encrypted		Yes	REP1

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)					
Hazardous Control Action: SiVES-C not provide send the voter's vote to SiVES-S when sives_s_authenticated_user is no and sives_s_available_status_ok is no (provided)					
Group 1 (Right Side): hazardous control action provided or safe control action required but not provided (issued)					
Interaction		**Elements**			
Vote (DF)		SiVES-S (Proc) and SiVES-C (Proc)			
Threat: 15. Potential Process Crash or Stop for SiVES-S					
Category: Denial Of Service					
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**	**Pertinent?**	**New or repeated?**
SiVES-S crashes, halts, stops or runs slowly; in all cases violating an availability metric.	Inadequate or insufficient resources allow denial of service	The system must have means to avoid DoS attack, like redundancy.		Yes	REP2
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them		Yes	REP2

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)	
Hazardous Control Action: SiVES-C not provide send the voter's vote to SiVES-S when sives_s_authenticated_user is no and sives_s_available_status_ok is no (provided)	
Group 1 (Right Side): hazardous control action provided or safe control action required but not provided (issued)	
Interaction	**Elements**
Vote (DF)	SiVES-S (Proc) and SiVES-C (Proc)
Threat: 16. Data Flow Generic Is Potentially Interrupted	
Category: Denial Of Service	

Scenarios	Associated Causal Factors	Requirements	Rationales	Pertinent?	New or repeated?
An external agent interrupts data flowing across a trust boundary in either direction.	Inadequate or insufficient resources allow denial of service	The system must have means to avoid DoS attack, like redundancy.		Yes	REP2
	Physical access to system installation for DoS actions	Protect physical installation		Yes	NEW

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)					
Hazardous Control Action: SiVES-C not provide send the voter's vote to SiVES-S when sives_s_authenticated_user is no and sives_s_available_status_ok is no (provided)					
Group 1 (Right Side): hazardous control action provided or safe control action required but not provided (issued)					
Interaction		**Elements**			
Vote (DF)		SiVES-S (Proc) and SiVES-C (Proc)			
Threat: 17. Elevation Using Impersonation					
Category: Elevation Of Privilege					
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**	**Pertinent?**	**New or repeated?**
SiVES-S may be able to impersonate the context of SiVES-C in order to gain additional privilege.	Incorrect or insecure configuration	System configuration must be revised and hardened		Yes	REP2
	Lack of training (competence) of system administrators, led to incorrect or insecure configurations	Administrators must be trained and have knowledge recycled regularly		Yes	REP2
	There is no user authenation on SiVES-S from SiVES-C	The system shall provide user authentication		Yes	REP2
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them		Yes	REP2

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)					
Hazardous Control Action: SiVES-C not provide send the voter's vote to SiVES-S when sives_s_authenticated_user is no and sives_s_available_status_ok is no (provided)					
Group 1 (Right Side): hazardous control action provided or safe control action required but not provided (issued)					
Interaction		**Elements**			
Vote (DF)		SiVES-S (Proc) and SiVES-C (Proc)			
Threat: 18. SiVES-S May be Subject to Elevation of Privilege Using Remote Code Execution					
Category: Elevation Of Privilege					
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**	**Pertinent?**	**New or repeated?**
SiVES-C may be able to remotely execute code for SiVES-S.	There is no user authenation on SiVES-S from SiVES-C	The system shall provide user authentication		Yes	REP2
	Inputs are not being validated	The input shall be validated		Yes	REP2
	Data injection modifies system behavior	The system shall have the latest update of antimalware and shall remove the malware		Yes	REP2
	Software not tested sufficiently before it goes into production	The application code must be thoroughly tested with the best methodologies before going into production		No	---
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them		Yes	NEW

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)					
Hazardous Control Action: SiVES-C not provide send the voter's vote to SiVES-S when sives_s_authenticated_user is no and sives_s_available_status_ok is no (provided)					
Group 1 (Right Side): hazardous control action provided or safe control action required but not provided (issued)					
Interaction		**Elements**			
Vote (DF)		SiVES-S (Proc) and SiVES-C (Proc)			
Threat: 19. Elevation by Changing the Execution Flow in SiVES-S					
Category: Elevation Of Privilege					
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**	**Pertinent?**	**New or repeated?**
An attacker may pass data into SiVES-S in order to change the flow of program execution within SiVES-S to the attacker's choosing.	Incorrect or insecure configuration	System configuration must be revised and hardened		Yes	REP2
	Lack of training (competence) of system administrators, led to incorrect or insecure configurations	Administrators must be trained and have knowledge recycled regularly		Yes	REP2
	Inputs are not being validated	The input shall be validated		Yes	REP2
	Data injection modifies system behavior	The system shall have the latest update of antimalware and shall remove the malware		Yes	REP2
	Software not tested sufficiently before it goes into production	The application code must be thoroughly tested with the best methodologies before going into production		Yes	REP2
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them		Yes	REP2

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)	
Hazardous Control Action: SiVES-C not provide send the voter's vote to SiVES-S when sives_s_authenticated_user is no and sives_s_available_status_ok is no (provided)	
Group 1 (Right Side): hazardous control action provided or safe control action required but not provided (issued)	
Interaction	**Elements**
Vote (DF)	SiVES-S (Proc) and SiVES-C (Proc)
Threat: 20. Cross Site Request Forgery	
Category: Elevation Of Privilege	

Scenarios	Associated Causal Factors	Requirements	Rationales	Pertinent?	New or repeated?
Cross-site request forgery (CSRF or XSRF) is a type of attack in which an attacker forces a user's browser to make a forged request to a vulnerable site by exploiting an existing trust relationship between the browser and the vulnerable web site. In a simple scenario, a user is logged in to web site A using a cookie as a credential. The other browses to web site B. Web site B returns a page with a hidden form that posts to web site A. Since the browser will carry the user's cookie to web site A, web site B now can take any action on web site A, for example, adding an admin to an account. The attack can be used to exploit any requests that the browser automatically authenticates, e.g. by session cookie, integrated authentication, IP whitelisting, ... The attack can be carried out in many ways such as by luring the victim to a site under control of the attacker, getting the user to click a link in a phishing email, or hacking a reputable web site that the victim will visit. The issue can only be resolved on the server side by requiring that all authenticated state-changing requests include an additional piece of secret payload (canary or CSRF token) which is known only to the legitimate web site and the browser and which is protected in transit through SSL/TLS. See the Forgery Protection property on the flow stencil for a list of mitigations.	Incorrect or insecure configuration	System configuration must be revised and hardened		Yes	REP2
	Lack of training (competence) of system administrators, led to incorrect or insecure configurations	Administrators must be trained and have knowledge recycled regularly		Yes	REP2
	There is no user authenation on SiVES-S from SiVES-C	The system shall provide user authentication		Yes	REP2
	Data carried over unencrypted connections or use weak encryption algorithms	All connections must be strongly encrypted		Yes	REP2
	Software not tested sufficiently before it goes into production	The application code must be thoroughly tested with the best methodologies before going into production		Yes	REP2
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them		Yes	REP2

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)					
Hazardous Control Action: SiVES-C not provide send the voter's vote to SiVES-S when sives_s_authenticated_user is no and sives_s_available_status_ok is no (provided)					
Group 1 (Right Side): hazardous control action provided or safe control action required but not provided (issued)					
Interaction		**Elements**			
Feedbacks from SiVES Servers to SiVES-S (DF)		SiVES-S (Proc) and SiVES Servers (Proc)			
Threat: 23. Cross Site Scripting					
Category: Tampering					
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**	**Pertinent?**	**New or repeated?**
The server 'SiVES-S' could be a subject to a cross-site scripting attack because it does not sanitize untrusted input.	Inputs are not being validated	The input shall be validated		Yes	REP2
	Data injection modifies system behavior	The system shall have the latest update of antimalware and shall remove the malware		Yes	REP2

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)					
Hazardous Control Action: SiVES-C not provide send the voter's vote to SiVES-S when sives_s_authenticated_user is no and sives_s_available_status_ok is no (provided)					
Group 1 (Right Side): hazardous control action provided or safe control action required but not provided (issued)					
Interaction		**Elements**			
Feedbacks from SiVES Servers to SiVES-S (DF)		SiVES-S (Proc) and SiVES Servers (Proc)			
Threat: 24. Elevation Using Impersonation					
Category: Elevation Of Privilege					
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**	**Pertinent?**	**New or repeated?**
SiVES-S may be able to impersonate the context of SiVES Servers in order to gain additional privilege.	Incorrect or insecure configuration	System configuration must be revised and hardened		Yes	REP2
	Lack of training (competence) of system administrators, led to incorrect or insecure configurations	Administrators must be trained and have knowledge recycled regularly		Yes	REP2
	There is no user authenation on SiVES-S from SiVES-C	The system shall provide user authentication		Yes	REP2
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them		Yes	REP2

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)					
Hazardous Control Action: SiVES-C not provide send the voter's vote to SiVES-S when sives_s_authenticated_user is no and sives_s_available_status_ok is no (provided)					
Group 1 (Right Side): hazardous control action provided or safe control action required but not provided (issued)					
Interaction		**Elements**			
Send IP Packets from SiVES Servers to Smartphone (DF)		SiVES Servers (Proc) and Smartphone (Proc)			
Threat: 37. Elevation Using Impersonation					
Category: Elevation Of Privilege					
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**	**Pertinent?**	**New or repeated?**
Smartphone may be able to impersonate the context of SiVES Servers in order to gain additional privilege.	Incorrect or insecure configuration	System configuration must be revised and hardened		Yes	REP2
	Lack of training (competence) of system administrators, led to incorrect or insecure configurations	Administrators must be trained and have knowledge recycled regularly		Yes	REP2
	There is no user authenation on SiVES-S from SiVES-C	The system shall provide user authentication		Yes	REP2
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them		Yes	REP2

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)					
Hazardous Control Action: SiVES-C not provide send the voter's vote to SiVES-S when sives_s_authenticated_user is no and sives_s_available_status_ok is no (provided)					
Group 1 (Right Side): hazardous control action provided or safe control action required but not provided (issued)					
Interaction		**Elements**			
Send IP Packets from SiVES Servers to Smartphone (DF)		SiVES Servers (Proc) and Smartphone (Proc)			
Threat: 38. Spoofing the SiVES Servers Process					
Category: Spoofing					
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**	**Pertinent?**	**New or repeated?**
SiVES Servers may be spoofed by an attacker and this may lead to unauthorized access to Smartphone. Consider using a standard authentication mechanism to identify the source process.	There is no user authenation on SiVES-S from SiVES-C	The system shall provide user authentication		Yes	REP2
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them		Yes	REP2

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)					
Hazardous Control Action: SiVES-C not provide send the voter's vote to SiVES-S when sives_s_authenticated_user is no and sives_s_available_status_ok is no (provided)					
Group 1 (Right Side): hazardous control action provided or safe control action required but not provided (issued)					
Interaction		**Elements**			
Send IP Packets from SiVES Servers to Smartphone (DF)		SiVES Servers (Proc) and Smartphone (Proc)			
Threat: 39. Spoofing the Smartphone Process					
Category: Spoofing					
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**	**Pertinent?**	**New or repeated?**
Smartphone may be spoofed by an attacker and this may lead to information disclosure by SiVES Servers. Consider using a standard authentication mechanism to identify the destination process.	There is no user authenation on SiVES-S from SiVES-C	The system shall provide user authentication		Yes	REP2
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them		Yes	REP2

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)					
Hazardous Control Action: SiVES-C not provide send the voter's vote to SiVES-S when sives_s_authenticated_user is no and sives_s_available_status_ok is no (provided)					
Group 1 (Right Side): hazardous control action provided or safe control action required but not provided (issued)					
Interaction		**Elements**			
Send IP Packets from SiVES Servers to Smartphone (DF)		SiVES Servers (Proc) and Smartphone (Proc)			
Threat: 40. Potential Data Repudiation by Smartphone					
Category: Repudiation					
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**	**Pertinent?**	**New or repeated?**
Smartphone claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.	Inadequate or inexistent service control and logs	Provide logs and auditing to ensure non-repudiation		Yes	REP2
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them		Yes	REP2

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)					
Hazardous Control Action: SiVES-C not provide send the voter's vote to SiVES-S when sives_s_authenticated_user is no and sives_s_available_status_ok is no (provided)					
Group 1 (Right Side): hazardous control action provided or safe control action required but not provided (issued)					
Interaction	**Elements**				
Send IP Packets from SiVES Servers to Smartphone (DF)	SiVES Servers (Proc) and Smartphone (Proc)				
Threat: 41. Potential Process Crash or Stop for Smartphone					
Category: Denial Of Service					
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**	**Pertinent?**	**New or repeated?**
Smartphone crashes, halts, stops or runs slowly; in all cases violating an availability metric.	Inadequate or insufficient resources allow denial of service	The system must have means to avoid DoS attack, like redundancy.		Yes	REP2
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them		Yes	REP2

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)					
Hazardous Control Action: SiVES-C not provide send the voter's vote to SiVES-S when sives_s_authenticated_user is no and sives_s_available_status_ok is no (provided)					
Group 1 (Right Side): hazardous control action provided or safe control action required but not provided (issued)					
Interaction		**Elements**			
Send IP Packets from SiVES Servers to Smartphone (DF)		SiVES Servers (Proc) and Smartphone (Proc)			
Threat: 42. Data Flow Send IP Packets from SiVES Servers to Smartphone Is Potentially Interrupted					
Category: Denial Of Service					
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**	**Pertinent?**	**New or repeated?**
An external agent interrupts data flowing across a trust boundary in either direction.	Inadequate or insufficient resources allow denial of service	The system must have means to avoid DoS attack, like redundancy.		Yes	REP2
	Physical access to system installation for DoS actions	Protect physical installation		Yes	REP2

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)					
Hazardous Control Action: SiVES-C not provide send the voter's vote to SiVES-S when sives_s_authenticated_user is no and sives_s_available_status_ok is no (provided)					
Group 1 (Right Side): hazardous control action provided or safe control action required but not provided (issued)					
Interaction		**Elements**			
Send IP Packets from SiVES Servers to Smartphone (DF)		SiVES Servers (Proc) and Smartphone (Proc)			
Threat: 43. Smartphone May be Subject to Elevation of Privilege Using Remote Code Execution					
Category: Elevation Of Privilege					
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**	**Pertinent?**	**New or repeated?**
SiVES Servers may be able to remotely execute code for Smartphone.	Incorrect or insecure configuration	System configuration must be revised and hardened		Yes	REP2
	Lack of training (competence) of system administrators, led to incorrect or insecure configurations	Administrators must be trained and have knowledge recycled regularly		Yes	REP2
	There is no user authenation on SiVES-S from SiVES-C	The system shall provide user authentication		Yes	REP2
	Inputs are not being validated	The input shall be validated		Yes	REP2
	Data injection modifies system behavior	The system shall have the latest update of antimalware and shall remove the malware		Yes	REP2
	Software not tested sufficiently before it goes into production	The application code must be thoroughly tested with the best methodologies before going into production		No	---
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them		Yes	REP2

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)					
Hazardous Control Action: SiVES-C not provide send the voter's vote to SiVES-S when sives_s_authenticated_user is no and sives_s_available_status_ok is no (provided)					
Group 1 (Right Side): hazardous control action provided or safe control action required but not provided (issued)					
Interaction		**Elements**			
Send IP Packets from SiVES Servers to Smartphone (DF)		SiVES Servers (Proc) and Smartphone (Proc)			
Threat: 44. Elevation by Changing the Execution Flow in Smartphone					
Category: Elevation Of Privilege					
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**	**Pertinent?**	**New or repeated?**
An attacker may pass data into Smartphone in order to change the flow of program execution within Smartphone to the attacker's choosing.	Inputs are not being validated	The input shall be validated		Yes	REP2
	Data injection modifies system behavior	The system shall have the latest update of antimalware and shall remove the malware		Yes	REP2
	Data injection modifies system behavior	The system shall have the latest update of antimalware and shall remove the malware		Yes	REP2
	Software not tested sufficiently before it goes into production	The application code must be thoroughly tested with the best methodologies before going into production		Yes	REP2
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them		Yes	REP2

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)					
Hazardous Control Action: SiVES-C not provide send the voter's vote to SiVES-S when sives_s_authenticated_user is no and sives_s_available_status_ok is no (provided)					
Group 1 (Right Side): hazardous control action provided or safe control action required but not provided (issued)					
Interaction		**Elements**			
Send IP Packets from SiVES Servers to Smartphone (DF)		SiVES Servers (Proc) and Smartphone (Proc)			
Threat: 45. Potential Lack of Input Validation for Smartphone					
Category: Tampering					
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**	**Pertinent?**	**New or repeated?**
Data flowing across Send IP Packets from SiVES Servers to Smartphone may be tampered with by an attacker. This may lead to a denial of service attack against Smartphone or an elevation of privilege attack against Smartphone or an information disclosure by Smartphone. Failure to verify that input is as expected is a root cause of a very large number of exploitable issues. Consider all paths and the way they handle data. Verify that all input is verified for correctness using an approved list input validation approach.	Inputs are not being validated	The input shall be validated		Yes	REP2
	Data injection modifies system behavior	The system shall have the latest update of antimalware and shall remove the malware		Yes	REP2

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)					
Hazardous Control Action: SiVES-C not provide send the voter's vote to SiVES-S when sives_s_authenticated_user is no and sives_s_available_status_ok is no (provided)					
Group 1 (Right Side): hazardous control action provided or safe control action required but not provided (issued)					
Interaction		**Elements**			
Send IP Packets from SiVES Servers to Smartphone (DF)		SiVES Servers (Proc) and Smartphone (Proc)			
Threat: 46. Data Flow Sniffing					
Category: Information Disclosure					
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**	**Pertinent?**	**New or repeated?**
Data flowing across Send IP Packets from SiVES Servers to Smartphone may be sniffed by an attacker. Depending on what type of data an attacker can read, it may be used to attack other parts of the system or simply be a disclosure of information leading to compliance violations. Consider encrypting the data flow.	There is no user authenation on SiVES-S from SiVES-C	The system shall provide user authentication		Yes	REP2
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them		Yes	REP2

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)					
Hazardous Control Action: SiVES-C not provide send the voter's vote to SiVES-S when sives_s_authenticated_user is no and sives_s_available_status_ok is no (provided)					
Group 1 (Right Side): hazardous control action provided or safe control action required but not provided (issued)					
Interaction		**Elements**			
Send IP Packets from Smartphone to SiVES Servers (DF)		SiVES Servers (Proc) and Smartphone (Proc)			
Threat: 47. Elevation Using Impersonation					
Category: Elevation Of Privilege					
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**	**Pertinent?**	**New or repeated?**
SiVES Servers may be able to impersonate the context of Smartphone in order to gain additional privilege.	Incorrect or insecure configuration	System configuration must be revised and hardened		Yes	REP2
	Lack of training (competence) of system administrators, led to incorrect or insecure configurations	Administrators must be trained and have knowledge recycled regularly		Yes	REP2
	There is no user authenation on SiVES-S from SiVES-C	The system shall provide user authentication		Yes	REP2
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them		Yes	REP2

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)					
Hazardous Control Action: SiVES-C not provide send the voter's vote to SiVES-S when sives_s_authenticated_user is no and sives_s_available_status_ok is no (provided)					
Group 1 (Right Side): hazardous control action provided or safe control action required but not provided (issued)					
Interaction		**Elements**			
Send IP Packets from Smartphone to SiVES Servers (DF)		SiVES Servers (Proc) and Smartphone (Proc)			
Threat: 48. Spoofing the Smartphone Process					
Category: Spoofing					
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**	**Pertinent?**	**New or repeated?**
Smartphone may be spoofed by an attacker and this may lead to unauthorized access to SiVES Servers. Consider using a standard authentication mechanism to identify the source process.	There is no user authenation on SiVES-S from SiVES-C	The system shall provide user authentication		Yes	REP2
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them		Yes	REP2

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)					
Hazardous Control Action: SiVES-C not provide send the voter's vote to SiVES-S when sives_s_authenticated_user is no and sives_s_available_status_ok is no (provided)					
Group 1 (Right Side): hazardous control action provided or safe control action required but not provided (issued)					
Interaction		**Elements**			
Send IP Packets from Smartphone to SiVES Servers (DF)		SiVES Servers (Proc) and Smartphone (Proc)			
Threat: 49. Spoofing the SiVES Servers Process					
Category: Spoofing					
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**	**Pertinent?**	**New or repeated?**
SiVES Servers may be spoofed by an attacker and this may lead to information disclosure by Smartphone. Consider using a standard authentication mechanism to identify the destination process.	There is no user authenation on SiVES-S from SiVES-C	The system shall provide user authentication		Yes	REP2
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them		Yes	REP2

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)					
Hazardous Control Action: SiVES-C not provide send the voter's vote to SiVES-S when sives_s_authenticated_user is no and sives_s_available_status_ok is no (provided)					
Group 1 (Right Side): hazardous control action provided or safe control action required but not provided (issued)					
Interaction	**Elements**				
Send IP Packets from Smartphone to SiVES Servers (DF)	SiVES Servers (Proc) and Smartphone (Proc)				
Threat: 50. Potential Data Repudiation by SiVES Servers					
Category: Repudiation					
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**	**Pertinent?**	**New or repeated?**
SiVES Servers claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.	Inadequate or inexistent service control and logs	Provide logs and auditing to ensure non-repudiation		Yes	REP2
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them		Yes	REP2

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)					
Hazardous Control Action: SiVES-C not provide send the voter's vote to SiVES-S when sives_s_authenticated_user is no and sives_s_available_status_ok is no (provided)					
Group 1 (Right Side): hazardous control action provided or safe control action required but not provided (issued)					
Interaction		**Elements**			
Send IP Packets from Smartphone to SiVES Servers (DF)		SiVES Servers (Proc) and Smartphone (Proc)			
Threat: 51. Potential Process Crash or Stop for SiVES Servers					
Category: Denial Of Service					
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**	**Pertinent?**	**New or repeated?**
SiVES Servers crashes, halts, stops or runs slowly; in all cases violating an availability metric.	Inadequate or insufficient resources allow denial of service	The system must have means to avoid DoS attack, like redundancy.		Yes	REP2
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them		Yes	REP2

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)	
Hazardous Control Action: SiVES-C not provide send the voter's vote to SiVES-S when sives_s_authenticated_user is no and sives_s_available_status_ok is no (provided)	
Group 1 (Right Side): hazardous control action provided or safe control action required but not provided (issued)	
Interaction	**Elements**
Send IP Packets from Smartphone to SiVES Servers (DF)	SiVES Servers (Proc) and Smartphone (Proc)
Threat: 52. Data Flow Send IP Packets from Smartphone to SiVES Servers Is Potentially Interrupted	
Category: Denial Of Service	

Scenarios	Associated Causal Factors	Requirements	Rationales	Pertinent?	New or repeated?
An external agent interrupts data flowing across a trust boundary in either direction.	Inadequate or insufficient resources allow denial of service	The system must have means to avoid DoS attack, like redundancy.		Yes	REP2
	Physical access to system installation for DoS actions	Protect physical installation		Yes	REP2

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)					
Hazardous Control Action: SiVES-C not provide send the voter's vote to SiVES-S when sives_s_authenticated_user is no and sives_s_available_status_ok is no (provided)					
Group 1 (Right Side): hazardous control action provided or safe control action required but not provided (issued)					
Interaction		**Elements**			
Send IP Packets from Smartphone to SiVES Servers (DF)		SiVES Servers (Proc) and Smartphone (Proc)			
Threat: 53. SiVES Servers May be Subject to Elevation of Privilege Using Remote Code Execution					
Category: Elevation Of Privilege					
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**	**Pertinent?**	**New or repeated?**
Smartphone may be able to remotely execute code for SiVES Servers.	Incorrect or insecure configuration	System configuration must be revised and hardened		Yes	REP2
	Lack of training (competence) of system administrators, led to incorrect or insecure configurations	Administrators must be trained and have knowledge recycled regularly		Yes	REP2
	There is no user authenation on SiVES-S from SiVES-C	The system shall provide user authentication		Yes	REP2
	Inputs are not being validated	The input shall be validated		Yes	REP2
	Data injection modifies system behavior	The system shall have the latest update of antimalware and shall remove the malware		Yes	REP2
	Software not tested sufficiently before it goes into production	The application code must be thoroughly tested with the best methodologies before going into production		Yes	REP2
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them		Yes	REP2

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)					
Hazardous Control Action: SiVES-C not provide send the voter's vote to SiVES-S when sives_s_authenticated_user is no and sives_s_available_status_ok is no (provided)					
Group 1 (Right Side): hazardous control action provided or safe control action required but not provided (issued)					
Interaction		**Elements**			
Send IP Packets from Smartphone to SiVES Servers (DF)		SiVES Servers (Proc) and Smartphone (Proc)			
Threat: 54. Elevation by Changing the Execution Flow in SiVES Servers					
Category: Elevation Of Privilege					
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**	**Pertinent?**	**New or repeated?**
An attacker may pass data into SiVES Servers in order to change the flow of program execution within SiVES Servers to the attacker's choosing.	Inputs are not being validated	The input shall be validated		Yes	REP2
	Data injection modifies system behavior	The system shall have the latest update of antimalware and shall remove the malware		Yes	REP2
	Data injection modifies system behavior	The system shall have the latest update of antimalware and shall remove the malware		Yes	REP2
	Software not tested sufficiently before it goes into production	The application code must be thoroughly tested with the best methodologies before going into production		Yes	REP2
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them		Yes	REP2

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)					
Hazardous Control Action: SiVES-C not provide send the voter's vote to SiVES-S when sives_s_authenticated_user is no and sives_s_available_status_ok is no (provided)					
Group 1 (Right Side): hazardous control action provided or safe control action required but not provided (issued)					
Interaction		**Elements**			
Send IP Packets from Smartphone to SiVES Servers (DF)		SiVES Servers (Proc) and Smartphone (Proc)			
Threat: 55. Potential Lack of Input Validation for SiVES Servers					
Category: Tampering					
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**	**Pertinent?**	**New or repeated?**
Data flowing across Send IP Packets from Smartphone to SiVES Servers may be tampered with by an attacker. This may lead to a denial of service attack against SiVES Servers or an elevation of privilege attack against SiVES Servers or an information disclosure by SiVES Servers. Failure to verify that input is as expected is a root cause of a very large number of exploitable issues. Consider all paths and the way they handle data. Verify that all input is verified for correctness using an approved list input validation approach.	Inputs are not being validated	The input shall be validated		Yes	REP2
	Data injection modifies system behavior	The system shall have the latest update of antimalware and shall remove the malware		Yes	REP2

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)					
Hazardous Control Action: SiVES-C not provide send the voter's vote to SiVES-S when sives_s_authenticated_user is no and sives_s_available_status_ok is no (provided)					
Group 1 (Right Side): hazardous control action provided or safe control action required but not provided (issued)					
Interaction		**Elements**			
Send IP Packets from Smartphone to SiVES Servers (DF)		SiVES Servers (Proc) and Smartphone (Proc)			
Threat: 56. Data Flow Sniffing					
Category: Information Disclosure					
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**	**Pertinent?**	**New or repeated?**
Data flowing across Send IP Packets from Smartphone to SiVES Servers may be sniffed by an attacker. Depending on what type of data an attacker can read, it may be used to attack other parts of the system or simply be a disclosure of information leading to compliance violations. Consider encrypting the data flow	There is no user authenation on SiVES-S from SiVES-C	The system shall provide user authentication		Yes	REP2
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them		Yes	REP2

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)					
Hazardous Control Action: SiVES-C not provide send the voter's vote to SiVES-S when sives_s_authenticated_user is no and sives_s_available_status_ok is no (provided)					
Group 1 (Right Side): hazardous control action provided or safe control action required but not provided (issued)					
Threats against: 93. Voter (EE)					
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**	**Pertinent?**	**New or repeated?**
Threats against the voter are related to coercion for the voter to vote for a candidate who offends the privacy of one or other specific voter. Despite this, this attack will not be considered, as it is very unlikely that it can be executed on a large scale, which could compromise the electronic voting system by the smartphone.				No	---

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)					
Hazardous Control Action: SiVES-C not provide send the voter's vote to SiVES-S when sives_s_authenticated_user is no and sives_s_available_status_ok is no (provided)					
Group 1 (Right Side): hazardous control action provided or safe control action required but not provided (issued)					
Threats against: 94. Smartphone (EE)					
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**	**Pertinent?**	**New or repeated?**
Voter and his/her vote exposed on a large scale	Malware infects large amount of smartphones to change its functioning and to leak information from the electronic voting system through each smartphone	SiVES must check if smartphone has updated anti-malware and just so to allow voting		Yes	REP1

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)					
Hazardous Control Action: SiVES-C not provide send the voter's vote to SiVES-S when sives_s_authenticated_user is no and sives_s_available_status_ok is no (provided)					
Group 1 (Right Side): hazardous control action provided or safe control action required but not provided (issued)					
Threats against: 94. Smartphone (EE)					
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**	**Pertinent?**	**New or repeated?**
Voters are prevented from voting	Malware in smartphones operating system leaks information	SiVES must check if smartphone has updated anti-malware and just so to allow voting		Yes	REP2

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)					
Hazardous Control Action: SiVES-C not provide send the voter's vote to SiVES-S when sives_s_authenticated_user is no and sives_s_available_status_ok is no (provided)					
Group 1 (Right Side): hazardous control action provided or safe control action required but not provided (issued)					
Threats against: 94. Smartphone (EE)					
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**	**Pertinent?**	**New or repeated?**
At any stage of the voting procedure, large number of voters claims that his/her vote was modified or disclosed by system error	Malware infects large amount of smartphones to change voter´s vote	SiVES must check if smartphone has updated anti-malware and just so to allow voting		Yes	REP2

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)					
Hazardous Control Action: SiVES-C not provide send the voter's vote to SiVES-S when sives_s_authenticated_user is no and sives_s_available_status_ok is no (provided)					
Group 1 (Right Side): hazardous control action provided or safe control action required but not provided (issued)					
Threats against: 95. SiVES-C (Proc)					
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**	**Pertinent?**	**New or repeated?**
The same threats against Smartphone				Yes	REP2

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)					
Hazardous Control Action: SiVES-C not provide send the voter's vote to SiVES-S when sives_s_authenticated_user is no and sives_s_available_status_ok is no (provided)					
Group 1 (Right Side): hazardous control action provided or safe control action required but not provided (issued)					
Threats against: 96. SiVES Servers (Proc)					
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**	**Pertinent?**	**New or repeated?**
The same threats against STI				No	---

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)					
Hazardous Control Action: SiVES-C not provide send the voter's vote to SiVES-S when sives_s_authenticated_user is no and sives_s_available_status_ok is no (provided)					
Group 1 (Right Side): hazardous control action provided or safe control action required but not provided (issued)					
Threats against: 97. SiVES-S (Proc)					
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**	**Pertinent?**	**New or repeated?**
The same threats against Smartphone by malware and/or intrusion and SiVES must check if smartphone has updated anti-malware and just so to allow voting and it must be checked continuously by Pentest Team and if a intrusion occurs the damages must be limited by a Computer Emergency Response Team – CERT.				Yes	REP2

Consolidate Losses

Control Action: Send the voter’s vote to SiVES-S (SiVES-C) (CA Nr 20)
Group 2 (Left Side): control action improperly executed or not executed

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)					
Group 2 (Left Side): control action improperly executed or not executed					
Interaction		**Elements**			
Commands from SiVES-C to Smartphone (DF)		SiVES-C (Proc) and Smartphone (Proc)			
Threat: 1. Spoofing the SiVES-C External Entity					
Category: Spoofing					
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**	**Pertinent?**	**New or repeated?**
SiVES-C may be spoofed by an attacker and this may lead to unauthorized access to Smartphone. Consider using a standard authentication mechanism to identify the external entity.	There is no user authenation on SiVES-S from SiVES-C	The system shall provide user authentication		Yes	REP2
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them		Yes	REP2

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)					
Group 2 (Left Side): control action improperly executed or not executed					
Interaction		**Elements**			
Commands from SiVES-C to Smartphone (DF)		SiVES-C (Proc) and Smartphone (Proc)			
Threat: 2. Elevation Using Impersonation					
Category: Elevation of Privilege					
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**	**Pertinent?**	**New or repeated?**
Smartphone may be able to impersonate the context of SiVES-C in order to gain additional privilege.	Incorrect or insecure configuration	System configuration must be revised and hardened		Yes	REP2
	Lack of training (competence) of system administrators, led to incorrect or insecure configurations			Yes	REP2
	There is no user authenation on SiVES-S from SiVES-C	The system shall provide user authentication		Yes	REP2
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them		Yes	REP2

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)					
Group 2 (Left Side): control action improperly executed or not executed					
Interaction		**Elements**			
Commands from SiVES-S to SiVES Servers (DF)		SiVES-S (Proc) and SiVES Servers (Proc)			
Threat: 3. Elevation Using Impersonation					
Category: Elevation of Privilege					
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**	**Pertinent?**	**New or repeated?**
SiVES Servers may be able to impersonate the context of SiVES-S in order to gain additional privilege.	Incorrect or insecure configuration	System configuration must be revised and hardened		Yes	REP2
	Lack of training (competence) of system administrators, led to incorrect or insecure configurations	Administrators must be trained and have knowledge recycled regularly		Yes	REP2
	There is no user authenation on SiVES-S from SiVES-C	The system shall provide user authentication		Yes	REP2
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them		Yes	REP2

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)	
Group 2 (Left Side): control action improperly executed or not executed	
Interaction	**Elements**
Commands from SiVES-S to SiVES Servers (DF)	SiVES-S (Proc) and SiVES Servers (Proc)
Threat: 3. Elevation Using Impersonation	
Category: Elevation of Privilege	

Scenarios	Associated Causal Factors	Requirements	Rationales	Pertinent?	New or repeated?
SiVES-C may be spoofed by an attacker and this may lead to information disclosure by SIVES-Sr using a standard authentication mechanism to identify the external entity.	There is no user authenation on SiVES-S from SiVES-C	The system shall provide user authentication		Yes	REP2
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them		Yes	REP2

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)	
Group 2 (Left Side): control action improperly executed or not executed	
Interaction	**Elements**
Feedbacks from SiVES-S to SiVES-C (DF)	SiVES-C (Proc) and SiVES-S (Proc)
Threat: 4. Spoofing of the SiVES-C External Destination Entity	
Category: Spoofing	

Scenarios	Associated Causal Factors	Requirements	Rationales	Pertinent?	New or repeated?
SiVES-C may be spoofed by an attacker and this may lead to information disclosure by SIVES-S	There is no user authenation on SiVES-S from SiVES-C	System must provide user authentication		No	---
	No cliente to server authentication and vice versa	The system shall provide authentication for both directions		No	---
	Presence of software bugs	The software shall be continuously tested and maintained.		No	---

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)					
Group 2 (Left Side): control action improperly executed or not executed					
Interaction		**Elements**			
Feedbacks from SiVES-S to SiVES-C (DF)		SiVES-C (Proc) and SiVES-S (Proc)			
Threat: 5. External Entity SiVES-C Potentially Denies Receiving Data					
Category: Repudiation					
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**	**Pertinent?**	**New or repeated?**
SiVES-C claims that it did not receive data from a process on the other side of the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.	Inadequate or inexistent service control and logs	Provide logs and auditing to ensure non-repudiation		Yes	REP1
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them		Yes	REP1

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)					
Hazardous Control Action: SiVES-C not provide send the voter's vote to SiVES-S when sives_s_authenticated_user is no and sives_s_available_status_ok is no (provided)					
Group 2 (Left Side): control action improperly executed or not executed					
Interaction		**Elements**			
Feedbacks from SiVES-S to SiVES-C (DF)		SiVES-C (Proc) and SiVES-S (Proc)			
Threat: 6. Data Flow Generic Is Potentially Interrupted					
Category: Denial Of Service					
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**	**Pertinent?**	**New or repeated?**
An external agent interrupts data flowing across a trust boundary in either direction.	Inadequate or insufficient resources allow denial of service	The system must have means to avoid DoS attack, like redundancy.		Yes	REP2
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them		Yes	REP2

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)	
Group 2 (Left Side): control action improperly executed or not executed	
Interaction	**Elements**
Vote (DF)	SiVES-S (Proc) and SiVES-C (Proc)
Threat: 9. Spoofing the SiVES-S Process	
Category: Spoofing	

Scenarios	Associated Causal Factors	Requirements	Rationales	Pertinent?	New or repeated?
SiVES-S may be spoofed by an attacker and this may lead to information disclosure by SiVES-C. Consider using a standard authentication mechanism to identify the destination process.	There is no user authenation on SiVES-S from SiVES-C	The system shall provide user authentication		Yes	REP2
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them		Yes	REP2

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)					
Group 2 (Left Side): control action improperly executed or not executed					
Interaction		**Elements**			
Vote (DF)		SiVES-S (Proc) and SiVES-C (Proc)			
Threat: 10. Spoofing the SiVES-C External Entity					
Category: Spoofing					
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**	**Pertinent?**	**New or repeated?**
SiVES-C may be spoofed by an attacker and this may lead to unauthorized access to SiVES-S. Consider using a standard authentication mechanism to identify the external entity.	There is no user authenation on SiVES-S from SiVES-C	The system shall provide user authentication		Yes	REP2
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them		Yes	REP2

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)					
Group 2 (Left Side): control action improperly executed or not executed					
Interaction		**Elements**			
Vote (DF)		SiVES-S (Proc) and SiVES-C (Proc)			
Threat: 11. Potential Lack of Input Validation for SiVES-S					
Category: Tampering					
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**	**Pertinent?**	**New or repeated?**
Data flowing across Vote may be tampered with by an attacker. This may lead to a denial of service attack against SiVES-S or an elevation of privilege attack against SiVES-S or an information disclosure by SiVES-S.	SiVES-S inputs is not validated	The input shall be validated		Yes	NEW
	Connection failure between SiVES-C and SiVES-S	Since the connection is made using Internet, nothing can be made. We assume that TCP handles the failure		No	---
	Intentional Tampering of data by external agent	The system shall provide message integrity check mechanism		Yes	NEW
	SiVES-C output is not validated	The output shall be validated		Yes	REP2
	Incorrect or insecure SiVES-S configuration	The SiVES-S configuration shall be reviewed and hardened.		Yes	REP2
	Lack of knowledge of system administrators that leads to incorrect or insecure settings	The system administrators shall be regularly recycled		No	REP2
	Presence of software bugs in SiVES-S and/or SiVES-C	The software shall be continuously tested and maintained.		Yes	REP2

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)					
Group 2 (Left Side): control action improperly executed or not executed					
Interaction		**Elements**			
Vote (DF)		SiVES-S (Proc) and SiVES-C (Proc)			
Threat: 12. Cross Site Scripting					
Category: Tampering					
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**	**Pertinent?**	**New or repeated?**
The server 'SiVES-S' could be a subject to a cross-site scripting attack because it does not sanitize untrusted input.	Inputs are not being validated	The input shall be validated		Yes	REP2
	Data injection modifies system behavior	The system shall have the latest update of antimalware and shall remove the malware		Yes	REP2

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)	
Group 2 (Left Side): control action improperly executed or not executed	
Interaction	**Elements**
Vote (DF)	SiVES-S (Proc) and SiVES-C (Proc)
Threat: 13. Potential Data Repudiation by SiVES-S	
Category: Repudiation	

Scenarios	Associated Causal Factors	Requirements	Rationales	Pertinent?	New or repeated?
SiVES-S claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.	Inadequate or inexistent service control and logs	Provide logs and auditing to ensure non-repudiation		Yes	REP2
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them		Yes	REP2

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)					
Group 2 (Left Side): control action improperly executed or not executed					
Interaction		**Elements**			
Vote (DF)		SiVES-S (Proc) and SiVES-C (Proc)			
Threat: 14. Data Flow Sniffing					
Category: Information Disclosure					
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**	**Pertinent?**	**New or repeated?**
Data flowing across Vote may be sniffed by an attacker. Depending on what type of data an attacker can read, it may be used to attack other parts of the system or simply be a disclosure of information leading to compliance violations. Consider encrypting the data flow.	Data carried over unencrypted connections or use weak encryption algorithms	All connections must be strongly encrypted		Yes	REP1

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)					
Group 2 (Left Side): control action improperly executed or not executed					
Interaction		**Elements**			
Vote (DF)		SiVES-S (Proc) and SiVES-C (Proc)			
Threat: 15. Potential Process Crash or Stop for SiVES-S					
Category: Denial Of Service					
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**	**Pertinent?**	**New or repeated?**
SiVES-S crashes, halts, stops or runs slowly; in all cases violating an availability metric.	Inadequate or insufficient resources allow denial of service	The system must have means to avoid DoS attack, like redundancy.		No	---
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them		No	---

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)					
Group 2 (Left Side): control action improperly executed or not executed					
Interaction		**Elements**			
Vote (DF)		SiVES-S (Proc) and SiVES-C (Proc)			
Threat: 16. Data Flow Generic Is Potentially Interrupted					
Category: Denial Of Service					
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**	**Pertinent?**	**New or repeated?**
An external agent interrupts data flowing across a trust boundary in either direction.	Inadequate or insufficient resources allow denial of service	The system must have means to avoid DoS attack, like redundancy.		Yes	REP2
	Physical access to system installation for DoS actions	Protect physical installation		Yes	REP2

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)					
Group 2 (Left Side): control action improperly executed or not executed					
Interaction		**Elements**			
Vote (DF)		SiVES-S (Proc) and SiVES-C (Proc)			
Threat: 17. Elevation Using Impersonation					
Category: Elevation Of Privilege					
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**	**Pertinent?**	**New or repeated?**
SiVES-S may be able to impersonate the context of SiVES-C in order to gain additional privilege.	Incorrect or insecure configuration	System configuration must be revised and hardened		Yes	REP2
	Lack of training (competence) of system administrators, led to incorrect or insecure configurations	Administrators must be trained and have knowledge recycled regularly		Yes	REP2
	There is no user authenation on SiVES-S from SiVES-C	The system shall provide user authentication		Yes	REP2
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them		Yes	REP2

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)	
Group 2 (Left Side): control action improperly executed or not executed	
Interaction	**Elements**
Vote (DF)	SiVES-S (Proc) and SiVES-C (Proc)
Threat: 18. SiVES-S May be Subject to Elevation of Privilege Using Remote Code Execution	
Category: Elevation Of Privilege	

Scenarios	Associated Causal Factors	Requirements	Rationales	Pertinent?	New or repeated?
SiVES-C may be able to remotely execute code for SiVES-S.	There is no user authenation on SiVES-S from SiVES-C	The system shall provide user authentication		Yes	REP2
	Inputs are not being validated	The input shall be validated		Yes	REP2
	Data injection modifies system behavior	The system shall have the latest update of antimalware and shall remove the malware		Yes	REP2
	Software not tested sufficiently before it goes into production	The application code must be thoroughly tested with the best methodologies before going into production		Yes	REP2
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them		Yes	REP2

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)					
Group 2 (Left Side): control action improperly executed or not executed					
Interaction		**Elements**			
Vote (DF)		SiVES-S (Proc) and SiVES-C (Proc)			
Threat: 19. Elevation by Changing the Execution Flow in SiVES-S					
Category: Elevation Of Privilege					
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**	**Pertinent?**	**New or repeated?**
An attacker may pass data into SiVES-S in order to change the flow of program execution within SiVES-S to the attacker's choosing.	Incorrect or insecure configuration	System configuration must be revised and hardened		Yes	REP2
	Lack of training (competence) of system administrators, led to incorrect or insecure configurations	Administrators must be trained and have knowledge recycled regularly		Yes	REP2
	Inputs are not being validated	The input shall be validated		Yes	REP2
	Data injection modifies system behavior	The system shall have the latest update of antimalware and shall remove the malware		Yes	REP2
	Software not tested sufficiently before it goes into production	The application code must be thoroughly tested with the best methodologies before going into production		Yes	REP2
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them		Yes	REP2

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)					
Group 2 (Left Side): control action improperly executed or not executed					
Interaction		**Elements**			
Vote (DF)		SiVES-S (Proc) and SiVES-C (Proc)			
Threat: 20. Cross Site Request Forgery					
Category: Elevation Of Privilege					
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**	**Pertinent?**	**New or repeated?**
Cross-site request forgery (CSRF or XSRF) is a type of attack in which an attacker forces a user's browser to make a forged request to a vulnerable site by exploiting an existing trust relationship between the browser and the vulnerable web site. In a simple scenario, a user is logged in to web site A using a cookie as a credential. The other browses to web site B. Web site B returns a page with a hidden form that posts to web site A. Since the browser will carry the user's cookie to web site A, web site B now can take any action on web site A, for example, adding an admin to an account. The attack can be used to exploit any requests that the browser automatically authenticates, e.g. by session cookie, integrated authentication, IP whitelisting, ... The attack can be carried out in many ways such as by luring the victim to a site under control of the attacker, getting the user to click a link in a phishing email, or hacking a reputable web site that the victim will visit. The issue can only be resolved on the server side by requiring that all authenticated state-changing requests include an additional piece of secret payload (canary or CSRF token) which is known only to the legitimate web site and the browser and which is protected in transit through SSL/TLS. See the Forgery Protection property on the flow stencil for a list of mitigations.	Incorrect or insecure configuration	System configuration must be revised and hardened		Yes	REP2
	Lack of training (competence) of system administrators, led to incorrect or insecure configurations	Administrators must be trained and have knowledge recycled regularly		Yes	REP2
	There is no user authenation on SiVES-S from SiVES-C	The system shall provide user authentication		Yes	REP2
	Data carried over unencrypted connections or use weak encryption algorithms	All connections must be strongly encrypted		Yes	REP2
	Software not tested sufficiently before it goes into production	The application code must be thoroughly tested with the best methodologies before going into production		Yes	REP2
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them		Yes	REP2

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)					
Group 2 (Left Side): control action improperly executed or not executed					
Interaction		**Elements**			
Feedbacks from SiVES Servers to SiVES-S (DF)		SiVES-S (Proc) and SiVES Servers (Proc)			
Threat: 23. Cross Site Scripting					
Category: Tampering					
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**	**Pertinent?**	**New or repeated?**
The server 'SiVES-S' could be a subject to a cross-site scripting attack because it does not sanitize untrusted input.	Inputs are not being validated	The input shall be validated		Yes	REP2
	Data injection modifies system behavior	The system shall have the latest update of antimalware and shall remove the malware		Yes	REP2

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)					
Group 2 (Left Side): control action improperly executed or not executed					
Interaction		**Elements**			
Feedbacks from SiVES Servers to SiVES-S (DF)		SiVES-S (Proc) and SiVES Servers (Proc)			
Threat: 24. Elevation Using Impersonation					
Category: Elevation Of Privilege					
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**	**Pertinent?**	**New or repeated?**
SiVES-S may be able to impersonate the context of SiVES Servers in order to gain additional privilege.	Incorrect or insecure configuration	System configuration must be revised and hardened		Yes	REP2
	Lack of training (competence) of system administrators, led to incorrect or insecure configurations	Administrators must be trained and have knowledge recycled regularly		Yes	REP2
	There is no user authenation on SiVES-S from SiVES-C	The system shall provide user authentication		Yes	REP2
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them		Yes	REP2

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)					
Group 2 (Left Side): control action improperly executed or not executed					
Interaction		**Elements**			
Send IP Packets from SiVES Servers to Smartphone (DF)		SiVES Servers (Proc) and Smartphone (Proc)			
Threat: 37. Elevation Using Impersonation					
Category: Elevation Of Privilege					
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**	**Pertinent?**	**New or repeated?**
Smartphone may be able to impersonate the context of SiVES Servers in order to gain additional privilege.	Incorrect or insecure configuration	System configuration must be revised and hardened		Yes	REP2
	Lack of training (competence) of system administrators, led to incorrect or insecure configurations	Administrators must be trained and have knowledge recycled regularly		Yes	REP2
	There is no user authenation on SiVES-S from SiVES-C	The system shall provide user authentication		Yes	REP2
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them		Yes	REP2

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)	
Group 2 (Left Side): control action improperly executed or not executed	
Interaction	**Elements**
Send IP Packets from SiVES Servers to Smartphone (DF)	SiVES Servers (Proc) and Smartphone (Proc)
Threat: 38. Spoofing the SiVES Servers Process	
Category: Spoofing	

Scenarios	Associated Causal Factors	Requirements	Rationales	Pertinent?	New or repeated?
SiVES Servers may be spoofed by an attacker and this may lead to unauthorized access to Smartphone. Consider using a standard authentication mechanism to identify the source process.	There is no user authenation on SiVES-S from SiVES-C	The system shall provide user authentication		Yes	REP2
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them		Yes	REP2

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)	
Group 2 (Left Side): control action improperly executed or not executed	
Interaction	**Elements**
Send IP Packets from SiVES Servers to Smartphone (DF)	SiVES Servers (Proc) and Smartphone (Proc)
Threat: 39. Spoofing the Smartphone Process	
Category: Spoofing	

Scenarios	Associated Causal Factors	Requirements	Rationales	Pertinent?	New or repeated?
Smartphone may be spoofed by an attacker and this may lead to information disclosure by SiVES Servers. Consider using a standard authentication mechanism to identify the destination process.	There is no user authenation on SiVES-S from SiVES-C	The system shall provide user authentication		Yes	REP2
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them		Yes	REP2

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)	
Group 2 (Left Side): control action improperly executed or not executed	
Interaction	**Elements**
Send IP Packets from SiVES Servers to Smartphone (DF)	SiVES Servers (Proc) and Smartphone (Proc)
Threat: 40. Potential Data Repudiation by Smartphone	
Category: Repudiation	

Scenarios	Associated Causal Factors	Requirements	Rationales	Pertinent?	New or repeated?
Smartphone claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.	Inadequate or inexistent service control and logs	Provide logs and auditing to ensure non-repudiation		Yes	REP2
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them		Yes	REP2

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)					
Group 2 (Left Side): control action improperly executed or not executed					
Interaction		**Elements**			
Send IP Packets from SiVES Servers to Smartphone (DF)		SiVES Servers (Proc) and Smartphone (Proc)			
Threat: 41. Potential Process Crash or Stop for Smartphone					
Category: Denial Of Service					
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**	**Pertinent?**	**New or repeated?**
Smartphone crashes, halts, stops or runs slowly; in all cases violating an availability metric.	Inadequate or insufficient resources allow denial of service	The system must have means to avoid DoS attack, like redundancy.		Yes	REP2
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them		Yes	REP2

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)	
Group 2 (Left Side): control action improperly executed or not executed	
Interaction	**Elements**
Send IP Packets from SiVES Servers to Smartphone (DF)	SiVES Servers (Proc) and Smartphone (Proc)
Threat: 42. Data Flow Send IP Packets from SiVES Servers to Smartphone Is Potentially Interrupted	
Category: Denial Of Service	

Scenarios	Associated Causal Factors	Requirements	Rationales	Pertinent?	New or repeated?
An external agent interrupts data flowing across a trust boundary in either direction.	Inadequate or insufficient resources allow denial of service	The system must have means to avoid DoS attack, like redundancy.		Yes	REP2
	Physical access to system installation for DoS actions	Protect physical installation		Yes	REP2

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)					
Group 2 (Left Side): control action improperly executed or not executed					
Interaction			**Elements**		
Send IP Packets from SiVES Servers to Smartphone (DF)			SiVES Servers (Proc) and Smartphone (Proc)		
Threat: 43. Smartphone May be Subject to Elevation of Privilege Using Remote Code Execution					
Category: Elevation Of Privilege					
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**	**Pertinent?**	**New or repeated?**
SiVES Servers may be able to remotely execute code for Smartphone.	Incorrect or insecure configuration	System configuration must be revised and hardened		Yes	REP2
	Lack of training (competence) of system administrators, led to incorrect or insecure configurations	Administrators must be trained and have knowledge recycled regularly		Yes	REP2
	There is no user authenation on SiVES-S from SiVES-C	The system shall provide user authentication		Yes	REP2
	Inputs are not being validated	The input shall be validated		Yes	REP2
	Data injection modifies system behavior	The system shall have the latest update of antimalware and shall remove the malware		Yes	REP2
	Software not tested sufficiently before it goes into production	The application code must be thoroughly tested with the best methodologies before going into production		Yes	REP2
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them		Yes	REP2

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)					
Group 2 (Left Side): control action improperly executed or not executed					
Interaction		**Elements**			
Send IP Packets from SiVES Servers to Smartphone (DF)		SiVES Servers (Proc) and Smartphone (Proc)			
Threat: 44. Elevation by Changing the Execution Flow in Smartphone					
Category: Elevation Of Privilege					
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**	**Pertinent?**	**New or repeated?**
An attacker may pass data into Smartphone in order to change the flow of program execution within Smartphone to the attacker's choosing.	Inputs are not being validated	The input shall be validated		Yes	REP2
	Data injection modifies system behavior	The system shall have the latest update of antimalware and shall remove the malware		Yes	REP2
	Data injection modifies system behavior	The system shall have the latest update of antimalware and shall remove the malware		Yes	REP2
	Software not tested sufficiently before it goes into production	The application code must be thoroughly tested with the best methodologies before going into production		Yes	REP2
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them		Yes	REP2

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)					
Group 2 (Left Side): control action improperly executed or not executed					
Interaction			**Elements**		
Send IP Packets from SiVES Servers to Smartphone (DF)			SiVES Servers (Proc) and Smartphone (Proc)		
Threat: 45. Potential Lack of Input Validation for Smartphone					
Category: Tampering					
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**	**Pertinent?**	**New or repeated?**
Data flowing across Send IP Packets from SiVES Servers to Smartphone may be tampered with by an attacker. This may lead to a denial of service attack against Smartphone or an elevation of privilege attack against Smartphone or an information disclosure by Smartphone. Failure to verify that input is as expected is a root cause of a very large number of exploitable issues. Consider all paths and the way they handle data. Verify that all input is verified for correctness using an approved list input validation approach.	Inputs are not being validated	The input shall be validated		Yes	REP2
	Data injection modifies system behavior	The system shall have the latest update of antimalware and shall remove the malware		Yes	REP2

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)					
Group 2 (Left Side): control action improperly executed or not executed					
Interaction		**Elements**			
Send IP Packets from SiVES Servers to Smartphone (DF)		SiVES Servers (Proc) and Smartphone (Proc)			
Threat: 46. Data Flow Sniffing					
Category: Information Disclosure					
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**	**Pertinent?**	**New or repeated?**
Data flowing across Send IP Packets from SiVES Servers to Smartphone may be sniffed by an attacker. Depending on what type of data an attacker can read, it may be used to attack other parts of the system or simply be a disclosure of information leading to compliance violations. Consider encrypting the data flow.	There is no user authenation on SiVES-S from SiVES-C	The system shall provide user authentication		Yes	REP2
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them		Yes	REP2

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)					
Group 2 (Left Side): control action improperly executed or not executed					
Interaction		**Elements**			
Send IP Packets from Smartphone to SiVES Servers (DF)		SiVES Servers (Proc) and Smartphone (Proc)			
Threat: 47. Elevation Using Impersonation					
Category: Elevation Of Privilege					
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**	**Pertinent?**	**New or repeated?**
SiVES Servers may be able to impersonate the context of Smartphone in order to gain additional privilege.	Incorrect or insecure configuration	System configuration must be revised and hardened		Yes	REP2
	Lack of training (competence) of system administrators, led to incorrect or insecure configurations	Administrators must be trained and have knowledge recycled regularly		Yes	REP2
	There is no user authenation on SiVES-S from SiVES-C	The system shall provide user authentication		Yes	REP2
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them		Yes	REP2

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)					
Group 2 (Left Side): control action improperly executed or not executed					
Interaction		**Elements**			
Send IP Packets from Smartphone to SiVES Servers (DF)		SiVES Servers (Proc) and Smartphone (Proc)			
Threat: 48. Spoofing the Smartphone Process					
Category: Spoofing					
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**	**Pertinent?**	**New or repeated?**
Smartphone may be spoofed by an attacker and this may lead to unauthorized access to SiVES Servers. Consider using a standard authentication mechanism to identify the source process.	There is no user authenation on SiVES-S from SiVES-C	The system shall provide user authentication		Yes	REP2
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them		Yes	REP2

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)					
Group 2 (Left Side): control action improperly executed or not executed					
Interaction		**Elements**			
Send IP Packets from Smartphone to SiVES Servers (DF)		SiVES Servers (Proc) and Smartphone (Proc)			
Threat: 49. Spoofing the SiVES Servers Process					
Category: Spoofing					
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**	**Pertinent?**	**New or repeated?**
SiVES Servers may be spoofed by an attacker and this may lead to information disclosure by Smartphone. Consider using a standard authentication mechanism to identify the destination process.	There is no user authenation on SiVES-S from SiVES-C	The system shall provide user authentication		Yes	REP2
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them		Yes	REP2

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)					
Group 2 (Left Side): control action improperly executed or not executed					
Interaction		**Elements**			
Send IP Packets from Smartphone to SiVES Servers (DF)		SiVES Servers (Proc) and Smartphone (Proc)			
Threat: 50. Potential Data Repudiation by SiVES Servers					
Category: Repudiation					
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**	**Pertinent?**	**New or repeated?**
SiVES Servers claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.	Inadequate or inexistent service control and logs	Provide logs and auditing to ensure non-repudiation		Yes	REP2
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them		Yes	REP2

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)	
Group 2 (Left Side): control action improperly executed or not executed	
Interaction	**Elements**
Send IP Packets from Smartphone to SiVES Servers (DF)	SiVES Servers (Proc) and Smartphone (Proc)
Threat: 51. Potential Process Crash or Stop for SiVES Servers	
Category: Denial Of Service	

Scenarios	Associated Causal Factors	Requirements	Rationales	Pertinent?	New or repeated?
SiVES Servers crashes, halts, stops or runs slowly; in all cases violating an availability metric.	Inadequate or insufficient resources allow denial of service	The system must have means to avoid DoS attack, like redundancy.		Yes	REP2
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them		Yes	REP2

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)					
Group 2 (Left Side): control action improperly executed or not executed					
Interaction		**Elements**			
Send IP Packets from Smartphone to SiVES Servers (DF)		SiVES Servers (Proc) and Smartphone (Proc)			
Threat: 52. Data Flow Send IP Packets from Smartphone to SiVES Servers Is Potentially Interrupted					
Category: Denial Of Service					
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**	**Pertinent?**	**New or repeated?**
An external agent interrupts data flowing across a trust boundary in either direction.	Inadequate or insufficient resources allow denial of service	The system must have means to avoid DoS attack, like redundancy.		Yes	REP2
	Physical access to system installation for DoS actions	Protect physical installation		Yes	REP2

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)					
Group 2 (Left Side): control action improperly executed or not executed					
Interaction		**Elements**			
Send IP Packets from Smartphone to SiVES Servers (DF)		SiVES Servers (Proc) and Smartphone (Proc)			
Threat: 53. SiVES Servers May be Subject to Elevation of Privilege Using Remote Code Execution					
Category: Elevation Of Privilege					
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**	**Pertinent?**	**New or repeated?**
Smartphone may be able to remotely execute code for SiVES Servers.	Incorrect or insecure configuration	System configuration must be revised and hardened		Yes	REP2
	Lack of training (competence) of system administrators, led to incorrect or insecure configurations	Administrators must be trained and have knowledge recycled regularly		Yes	REP2
	There is no user authenation on SiVES-S from SiVES-C	The system shall provide user authentication		Yes	REP2
	Inputs are not being validated	The input shall be validated		Yes	REP2
	Data injection modifies system behavior	The system shall have the latest update of antimalware and shall remove the malware		Yes	REP2
	Software not tested sufficiently before it goes into production	The application code must be thoroughly tested with the best methodologies before going into production		Yes	REP2
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them		Yes	REP2

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)					
Group 2 (Left Side): control action improperly executed or not executed					
Interaction			**Elements**		
Send IP Packets from Smartphone to SiVES Servers (DF)			SiVES Servers (Proc) and Smartphone (Proc)		
Threat: 54. Elevation by Changing the Execution Flow in SiVES Servers					
Category: Elevation Of Privilege					
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**	**Pertinent?**	**New or repeated?**
An attacker may pass data into SiVES Servers in order to change the flow of program execution within SiVES Servers to the attacker's choosing.	Inputs are not being validated	The input shall be validated		Yes	REP2
	Data injection modifies system behavior	The system shall have the latest update of antimalware and shall remove the malware		Yes	REP2
	Data injection modifies system behavior	The system shall have the latest update of antimalware and shall remove the malware		Yes	REP2
	Software not tested sufficiently before it goes into production	The application code must be thoroughly tested with the best methodologies before going into production		Yes	REP2
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them		Yes	REP2

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)					
Group 2 (Left Side): control action improperly executed or not executed					
Interaction			**Elements**		
Send IP Packets from Smartphone to SiVES Servers (DF)			SiVES Servers (Proc) and Smartphone (Proc)		
Threat: 55. Potential Lack of Input Validation for SiVES Servers					
Category: Tampering					
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**	**Pertinent?**	**New or repeated?**
Data flowing across Send IP Packets from Smartphone to SiVES Servers may be tampered with by an attacker. This may lead to a denial of service attack against SiVES Servers or an elevation of privilege attack against SiVES Servers or an information disclosure by SiVES Servers. Failure to verify that input is as expected is a root cause of a very large number of exploitable issues. Consider all paths and the way they handle data. Verify that all input is verified for correctness using an approved list input validation approach.	Inputs are not being validated	The input shall be validated		Yes	REP2
	Data injection modifies system behavior	The system shall have the latest update of antimalware and shall remove the malware		Yes	REP2

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)					
Group 2 (Left Side): control action improperly executed or not executed					
Interaction		**Elements**			
Send IP Packets from Smartphone to SiVES Servers (DF)		SiVES Servers (Proc) and Smartphone (Proc)			
Threat: 56. Data Flow Sniffing					
Category: Information Disclosure					
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**	**Pertinent?**	**New or repeated?**
Data flowing across Send IP Packets from Smartphone to SiVES Servers may be sniffed by an attacker. Depending on what type of data an attacker can read, it may be used to attack other parts of the system or simply be a disclosure of information leading to compliance violations. Consider encrypting the data flow	There is no user authenation on SiVES-S from SiVES-C	The system shall provide user authentication		Yes	REP2
	Presence of software bugs	The development must be cyclic and constant to search fault and correct them		Yes	REP2

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)					
Group 2 (Left Side): control action improperly executed or not executed					
Threats against: 93. Voter (EE)					
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**	**Pertinent?**	**New or repeated?**
Threats against the voter are related to coercion for the voter to vote for a candidate who offends the privacy of one or other specific voter. Despite this, this attack will not be considered, as it is very unlikely that it can be executed on a large scale, which could compromise the electronic voting system by the smartphone.				No	---

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)					
Group 2 (Left Side): control action improperly executed or not executed					
Threats against: 94. Smartphone (EE)					
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**	**Pertinent?**	**New or repeated?**
Voter and his/her vote exposed on a large scale	Malware infects large amount of smartphones to change its functioning and to leak information from the electronic voting system through each smartphone	SiVES must check if smartphone has updated anti-malware and just so to allow voting		Yes	REP2

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)					
Group 2 (Left Side): control action improperly executed or not executed					
Threats against: 94. Smartphone (EE)					
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**	**Pertinent?**	**New or repeated?**
Voters are prevented from voting	Malware in smartphones operating system leaks information	SiVES must check if smartphone has updated anti-malware and just so to allow voting		Yes	NEW

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)					
Group 2 (Left Side): control action improperly executed or not executed					
Threats against: 94. Smartphone (EE)					
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**	**Pertinent?**	**New or repeated?**
At any stage of the voting procedure, large number of voters claims that his/her vote was modified or disclosed by system error	Malware infects large amount of smartphones to change voter´s vote	SiVES must check if smartphone has updated anti-malware and just so to allow voting		Yes	REP2

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)					
Group 2 (Left Side): control action improperly executed or not executed					
Threats against: 95. SiVES-C (Proc)					
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**	**Pertinent?**	**New or repeated?**
The same threats against Smartphone				Yes	REP2

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)					
Group 2 (Left Side): control action improperly executed or not executed					
Threats against: 96. SiVES Servers (Proc)					
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**	**Pertinent?**	**New or repeated?**
The same threats against STI				No	---

Consolidate Losses

Control Action: Send the voter's vote to SiVES-S (SiVES-C) (CA Nr 20)					
Group 2 (Left Side): control action improperly executed or not executed					
Threats against: 97. SiVES-S (Proc)					
Scenarios	**Associated Causal Factors**	**Requirements**	**Rationales**	**Pertinent?**	**New or repeated?**
The same threats against Smartphone by malware and/or intrusion and SiVES must check if smartphone has updated anti-malware and just so to allow voting and it must be checked continuously by Pentest Team and if a intrusion occurs the damages must be limited by a Computer Emergency Response Team – CERT.				Yes	REP2

Process to identify the security requirements - Overview

The process to identify the security requirements **WAS**:

- Execute steps 1, 2 and 3
- Execute activities 4.1 and 4.2 from STPA Step 4
- Map model elements and obtain the DFD (DIEFD) from CS (Task 4.3.1)
- Identify threats and vulnerabilities in DIEFD (STRIDE Analysis) (Task 4.3.2)
- Identify scenarios (Task 4.3.3)
- Consolidate Losses (Activity 4.4): for each HCA, verify which 3-tuple can be a causal factor. If it can be, generate a requirement (recommendation) with redundancy check (NEW and REP states)

Steps 1, 2 and 3 – Summary

Overview Data Analysis – General Results **before** STPA extension with STRIDE (without Step 4)

INFORMATIONS	QUANTITY
Unacceptable Losses	3
Hazards	7
Constraints	8
Control Actions	28
Hazardous Control Actions	63
Controller Constraints	63

Activities 4.1 and 4.2 – Summary

Results to **one** Control Action (CA Nr 20) and to **one** Hazardous Control Action **before** STPA extension with STRIDE (Activities 4.1 and 4.2)

INFORMATIONS	QUANTITY
Scenarios (Sce)	17
Requirements (Req)	17

Results to **one** Control Action (CA Nr 20) and to **one** Hazardous Control Action **after** STPA extension with STRIDE (Activities 4.1 to 4.4)

INFORMATIONS	QUANTITY
Scenarios (Sce)	17 **+ 9**
Requirements (Req)	17 **+ 12**

Conclusions

The confrontation of the STRIDE attack scenarios must be done for each CA and HCA raised by Activities 4.1 and 4.2, which greatly expands the possibility of finding unexpected causal factors or difficult to detect.

Even if there is a scenario, both in Activities 4.1 and 4.2 and in STRIDE, it can be merged to specialize this scenario under aspects of security which in itself is already an important improvement of the analysis itself.

The presented model reveals new scenarios through extension with STRIDE, enhances existing scenarios, and removes redundancies or repetitions.

Finally, recommendations will be derived from Requirements of Activities 4.1 and 4.2 Analysis and Approved Requirements of Consolidate Losses (pertinent + check redundancy) found in these analysis.

The STRIDE model does not replace Activities 4.1 and 4.2 of the STPA, but **complements it** by increasing the focus on cybersecurity in order to make the analysis more complete as a whole.