ALMA MATER STUDIORUM - UNIVERSITÀ DI BOLOGNA
SEDE DI CESENA
SECONDA FACOLTÀ DI INGEGNERIA CON SEDE A CESENA
CORSO DI LAUREA SPECIALISTICA IN INGEGNERIA INFORMATICA

ANALISI DELLA SICUREZZA DEI PROCESSI DI VOTO ELETTRONICO

Tesi in

Sistemi e Tecnologie per la Sicurezza LS

Relatore:
Prof. Franco Callegati

Presentata da:
Andrea Leoni

Correlatori:
Prof. Marco Prandini

Sessione II

Anno Accademico 2011/2012

Indice

Introduzione

La capacità di portare avanti elezioni corrette è stata sempre considerata un punto fondamentale della democrazia. In passato ci sono stati tentativi di frode o manipolazione dei voti, così come ci sono stati tentativi di utilizzare approcci tecnologici per cercare di rendere l'elezione sicura e corretta. Recentemente questi tentativi si sono focalizzati su due tecnologie principali, macchine DRE (Direct Recording Electronic) e internet voting. Le macchine DRE permettono di esprimere il voto in modo elettronico al seggio, l'internet voting permette di votare da una qualsiasi macchina collegata alla rete. Oltre al modo in cui esprimere il voto, però, un'elezione è composta da molto altro, come la creazione di un registro degli elettori, l'autenticazione, e tutte le altre attività legate all'elezione stessa. L'insieme di queste attività è detto processo di voto.

In questa tesi verranno presentata una metodologia, già utilizzata negli Stati Uniti per modellare il processo di voto di Yolo County in California, per modellare un processo di voto e verificare la presenza di vulnerabilità al suo interno. Questa metodologia sarà poi applicata a un processo di voto elettronico europeo, quello utilizzato in Norvegia, che sarà analizzato in cerca di vulnerabilità, con il duplice obiettivo di verificare il suo livello di robustezza contro una specifica minaccia e di verificare anche se la metodologia presentata può essere applicata con successo anche ad altri processi oltre quello californiano. Inoltre in base al risultato dell'analisi del processo si cercherà di proporre un miglioramento in modo da renderlo più sicuro.

Organizzazione della tesi

Il capitolo 1 offre una panoramica generale sull'e-voting, dando una spiegazione del concetto, fornendo una panoramica dei principali tipi di tecnologie impiegate per il voto elettronico e spiegando cosa dovrebbe garantire un corretto sistema di e-voting.

Il capitolo 2 contiene una definizione del termine processo di voto, spiegando da cosa è composto un processo e perchè è importante esaminarlo nel suo insieme. Vengono poi presentati i processi di voto di alcuni Paesi europei, Norvegia, Olanda, Estonia e Svizzera, ognuno avente le sue caratteristiche.

Il capitolo 3 spiega quali strumenti di modellazione e analisi sono stati utilizzati per il processo di voto di Yolo County, e che saranno utilizzati nel capitolo 4 per il caso di studio di questa tesi. Viene spiegato il linguaggio Little-JIL e la sua semantica, e viene spiegata la Fault Tree Analysis.

Il capitolo 4 presenta un caso di studio, la modellazione e analisi del processo di voto norvegese per mezzo degli strumenti introdotti nel capitolo 3. Il capitolo spiega la metodologia utilizzata, presenta il modello del processo che si è ottenuto, mostra i risultati dell'analisi effettuata su tale modello e propone un miglioramento. Alla fine vengono presentati i risultati e proposte alcune considerazioni e sviluppi futuri.

Capitolo 1

E-Voting

In questo capitolo viene offerta una panoramica generale sull'e-voting e sulle principali tecnologie utilizzate nei sistemi di voto elettronico.

1.1 Cos'è

L'elezione, in ognuno dei suoi livelli, è una parte fondamentale di qualsiasi stato democratico, perché attraverso di essa si ha la possibilità di scegliere chi ne sarà alla guida. Data la sua importanza, si è sempre cercato di svolgerla nel modo più corretto e sicuro possibile, dando la possibilità di esprimere il voto in modo chiaro e non ambiguo, e cercando di garantire i principi base che la regolano, come ad esempio non rendere possibile che un elettore voti più volte, oppure verificare che il numero di voti espressi in un seggio sia uguale al numero di elettori che hanno votato in quel seggio. I sistemi di voto si sono storicamente basati sull'utilizzo della carta: un elettore si recava al seggio elettorale e il voto veniva espresso su una scheda cartacea segnando il simbolo corrispondente alla parte politica a cui si voleva destinare il proprio voto, e la conta di tutti i voti per determinare i risultati veniva svolta a mano. Nonostante in molti Paesi questo sistema sia ancora quello ufficiale, nell'era dell'informazione è quasi doverosa l'idea di utilizzare la tecnologia a

disposizione per facilitare alcune parti di questo metodo di scelta dei rappresentanti, per renderlo meno suscettibile ad eventuali errori umani. Con il termine voto elettronico (detto anche e-voting) ci si riferisce ad un utilizzo della tecnologia durante un'elezione, in modo tale che l'espressione della scelta durante il voto, la registrazione del voto, il conteggio, la presentazione dei risultati ed eventualmente la loro trasmissione sia effettuato tramite una macchina.

1.2 Tipi

Questa unione tra voto e tecnologia è iniziata nel 1960, dove più che di vero e proprio e-voting si trattava di conteggio elettronico (e-counting): una macchina, grazie a uno scanner ottico, riconosceva la preferenza espressa dal segno sulla scheda e registrava il voto. Oggi la situazione si è ovviamente evoluta, ed esistono due metodi principali di voto elettronico: voto tramite DRE e Internet Voting [14].

1.2.1 DRE

DRE (Direct Recording Electronic) è una macchina che tramite un display fornisce una versione digitale della scheda elettorale con la quale l'elettore può interagire per esprimere il proprio voto (ad esempio tramite bottoni o touchscreen), e che registra il voto espresso in un componente di memoria. Finita l'elezione la macchina produce un documento in cui riporta in forma tabellare i voti che aveva memorizzato al proprio interno (questo documento può essere stampato o presente su una memoria rimovibile). A seconda dei casi può anche fornire un modo per trasmettere i voti a un server centrale in cui vengono aggregati tutti i voti provenienti dai vari seggi. La macchina è posta all'interno del seggio, all'interno della più classica cabina elettorale. Un elettore, dopo essersi autenticato al seggio tramite le modalità stabilite dallo stato, può andare a esprimere la propria scelta tramite la macchina.

Uno dei punti che rendono difficile da parte di un elettore fidarsi di una macchina DRE è che non è possibile da parte sua vedere o verificare le operazioni svolte durante e dopo l'azione di voto. Una buona norma dunque è quella di avere macchine che producano una traccia cartacea per la verifica da parte dell'elettore, in modo da mostrare che il voto è stato registrato e con quale scelta.

Degno di nota è il fatto che utilizzando macchine DRE all'interno dei seggi si può rendere più facile il voto a persone con disabilità. Queste macchine infatti possono essere rese pienamente accessibili per chiunque, integrando in esse varie tecnologie come cuffie, pedali, o sistemi sip&puff, solo per citarne alcuni.

1.2.2 Internet voting

Un'altro metodo di voto elettronico è il voto tramite Internet, chiamato anche internet voting o i-voting. Questa metodologia permette all'elettore di esprimere la sua preferenza durante il voto tramite una qualsiasi macchina connessa alla rete. Solitamente, a questo scopo, viene creato un sito internet apposito a cui l'elettore si deve collegare in un periodo di tempo stabilito dall'organo che si occupa di stilare le regole per l'elezione, che può andare da un arco di 30 giorni prima del giorno dell'elezione a poche ore del giorno stesso. Una volta raggiunto il sito deve superare una fase di identificazione, durante la quale da prova della propria identità (tramite ad esempio una ID card nazionale, oppure tramite codici forniti alla persona dallo stato) e può poi esprimere la sua scelta di voto. L'autenticazione nell'internet voting è una parte importante, in quanto viene a mancare il riconoscimento al seggio elettorale ed è quindi necessario avere un forte sistema di conferma dell'identità.

L'internet voting può essere implementato anche tramite macchine connesse ad Internet all'interno del seggio elettorale se l'organizzazione dell'elezione lo permette o lo richiede. Questo sistema però toglie quello che può

essere visto come il più grande vantaggio dell'i-voting, ossia il voto da remoto, che permette di partecipare con facilità all'elezione anche ai cittadini residenti in altre parti del mondo.

Questo sistema si può considerare l'evoluzione del voto tramite posta, già utilizzato da diversi Paesi.

1.3 Caratteristiche

Il tradizionale voto basato su carta ottiene la fiducia dell'elettore attraverso la diretta interazione tra chi vota e le autorità elettorali del seggio, e anche tramite la parte fisica che rimane, ossia la scheda elettorale. La segretezza e integrità del voto sono garantite dal mettere la scheda, anonima, nell'urna che verrà aperta solo in fase di conteggio. Il conteggio a sua volta è percepito come corretto grazie alla presenza di persone di interessi politici diversi. Inoltre spesso vengono usati sistemi di identificazione del votante al seggio, in modo da impedire che uno stesso elettore voti due, o più, volte.

L'e-voting porta le procedure del voto cartaceo in un sistema elettronico che le simula e che deve essere in grado di garantire le stesse caratteristiche. Deve quindi essere impossibile, partendo da una scheda elettorale elettronica inviata, risalire all'identità del votante, in modo da capire chi ha votato cosa. Deve parimenti essere impossibile che i voti espressi elettronicamente vengano alterati, ma devono invece essere immagazzinati esattamente come scelti dal votante e rimanere tali. Deve inoltre esserci una qualche misura di autenticazione, in modo che un singolo elettore possa votare soltanto una volta, esattamente come nel voto tramite scheda cartacea.

1.4 Considerazioni

Dopo quanto detto, risulta evidente che l'utilizzo dell'e-voting introduca alcuni vantaggi, come il facile accesso alla procedura di voto anche per chi si trova all'estero o per chi non può recarsi al seggio, o la facilitazione del conteggio ed esclusione di errori umani da esso. Insieme ai vantaggi vengono però alcuni possibili lati negativi: ad esempio in alcuni sistemi, soprattutto di voto tramite internet, potrebbe essere facilitato il vote buying, ossia la compravendita di voti, o il voto familiare, in cui un membro della famiglia autoritario impone il proprio voto agli altri.

Gli aspetti negativi appena citati possono essere contenuti costruendo un processo di voto robusto.

Capitolo 2

Processi di voto

In questo capitolo viene data la definizione di quello che è chiamato processo di voto o elettorale, e viene data una panoramica di alcuni dei processi elettorali di voto elettronico utilizzati in Europa.

2.1 Cos'è un processo di voto

Un'elezione, come definita in [18], è la scelta formale di una persona per un incarico, impiego o posizione di qualsiasi tipo; solitamente tramite il voto di un corpo elettorale. Tale scelta richiede un processo, o una sequenza di azioni, che risulti in una selezione. Questo processo può essere semplice come contare le mani alzate in una stanza, o complesso come contare i voti attraverso una molteplicità di giurisdizioni, ognuna delle quali usa le sue proprie regole per rendere i voti disponibili. Effettivamente, parte del processo è determinare QUALI voti contare, e chi è un membro del corpo elettorale. Le regole che governano tutto ciò sono essenzialmente una questione politico, perché a differenti tipi di elezioni si applicano differenti regole. Una parte ugualmente importante del processo elettorale è la validazione dei risultati, per confermare che i voti sono stati contati correttamente. Qui il grado di certezza nella correttezza del risultato e la selezione del metodo usato per

effettuare la validazione sono entrambi questioni politiche, tuttavia come il metodo scelto è implementato non è una questione politica, ma piuttosto una tecnica.

Il processo è importante perché i risultati di un'elezione possono avere effetti sul corso della storia, e più nell'immediato sulla vita dei cittadini e sui rapporti internazionali. Un processo elettorale coinvolge persone. Presidenti del seggio, candidati, scrutatori, elettori tutti partecipano direttamente nel processo. Meno direttamente partecipano anche legislatori, e chiunque altro decida le regole relative a chi può votare e come l'elezione deve svolgersi. Le regole possono essere complicate, specialmente quando una singola scheda include competizioni politiche per diverse giurisdizioni, ognuna con le proprie regole. Ad esempio in alcuni Paesi può accadere che nella stessa scheda si voti per una scelta a livello nazionale e una a livello locale, e che i voti vengano contati in modo differente per determinare i risultati nelle due diverse giurisdizioni.

Meno ovvio ma non meno serio è il fatto che sorgano problemi durante il processo di voto. Per esempio, un'urna elettorale può non essere restituita quando richiesto, o dei voti possono essere conteggiati due volte. Questi problemi possono essere individuati rapidamente se vengono anticipati, quando presidenti di seggio con esperienza prendono provvedimenti per la loro identificazione e correzione. Nonostante molti distretti elettorali abbiano adottato provvedimenti per gestire problemi conosciuti, può sempre capitare il presentarsi di problemi sconosciuti. Attualmente, i presidenti di seggio usano approcci ad hoc sia per affrontare i problemi quando si presentano che per anticiparli prima che sorgano.

2.2 Processi di voto elettronico in europa

Di seguito vengono presentati i processi di voto utilizzati in Norvegia nel 2011, in Olanda nel 2006, in Estonia nel 2007 e in Svizzera nel 2011.

2.2.1 Norvegia

L'elezione svoltasi in Norvegia nel 2011 [9], per l'elezione di governi locali, ha trovato spazio al proprio interno per un esperimento riguardante l'e-voting, in particolare l'internet voting [2]. Dieci comuni norvegesi hanno dato la possibilità ai propri elettori, sia all'estero che su suolo nazionale, di votare tramite un apposito servizio web.

Di seguito vengono presentati gli organi che si occupano della gestione delle elezioni, e viene illustrato l'intero processo elettorale.

Organi

L'amministrazione dell'elezione in Norvegia ha diversi livelli, tra cui il National Electoral Commitee (non presente nelle elezioni 2011 in quanto elezioni locali e non nazionali), County Electoral Commitees, Electoral Committees a livello municipale e i Polling Committees ai seggi elettorali. Ad ogni modo, la struttura opera come gerarchia durante il processo di conteggio dei voti, e le responsabilità per la maggior parte degli aspetti dell'amministrazione elettorale sono concentrate a livello municipale, con l'amministrazione comunale che si occupa della maggior parte dell'organizzazione.

County Electoral Commitee. I 19 CECs approvano le liste elettorali, stampano le schede elettorali, verificano la tabulazione dei voti delle municipalità e assegnano i seggi ai candidati eletti nella circoscrizione. Ogni CEC è eletto dal County Council, la cui composizione politica è riportata nel CEC.

Electoral Commitee. i 430 ECs hanno la responsabilità generale riguardo l'organizzare e lo far svolgere l'elezione nelle rispettive municipalità. Ogni EC è eletto diversi mesi prima del giorno dell'elezione dal consiglio municipale, la cui composizione politica è riportata nell'EC. Il numero dei membri non è fissato. Mentre gli ECs sono organi decisionali, l'amministrazione municipale porta avanti la maggior parte delle questioni

organizzative relative all'elezione. L'EC è anche coinvolto nel processo di conteggio scannerizzando tutti i voti e confrontando il totale con i risultati calcolati a mano nelle polling station.

Polling Committee. PCs sono responsabili di amministrare l'elezione nelle polling station il giorno dell'elezione stessa (tranne nelle municipalità con una sola polling station, in quel caso se ne occupa l'EC). I PCs sono selezionati dal cosiglio municipale, anche se la responsabilità può essere delegata all'EC. Ogni PC ha almeno 3 membri. Contano i voti dati il giorno dell'elezione, mentre l'EC conta quelli dati durante il periodo di advanced voting. Il leader di un PC e il capo dei lavoratori della polling station condividono le responsabilità per gestire la polling station.

Registrazioni

In Norvegia c'è un sistema di registrazione degli elettori continuo e passivo. Il registro degli elettori è preso dal registro civile, che è amministrato dalla Population Registry Authority (non ho dettagli di scadenza 2011). Gli ECs sono responsabili di custodire il registro degli elettori una volta creato, e di distribuire in ciascuna municipalità le polling cards (che servono per informare gli elettori in quale polling station sono registrati per votare) agli elettori aventi diritto al voto. Il registro degli elettori è reso pubblico in ogni municipalità, e gli elettori possono richiedere correzioni fino al giorno dell'elezione. Le correzioni che possono essere applicate al registro dalle autorità municipali includono l'inserimento di cittadini che vivono all'estero, notifiche di persone che vivevano all'estero e sono tornate in Norvegia, correzione di errori, nuovi cittadini, e rimozione dei nomi di persone decedute.

Per quanto riguarda la registrazione delle liste di candidati, il termine per la loro presentazione è 31 marzo dell'anno delle elezioni. Le liste a livello di contea devono essere proposte con un sostegno di almeno 500 firme di elettori aventi diritto al voto nell'elezione corrente. A livello municipale le firme devono essere il 2% degli abitanti che avevano diritto di voto all'elezione

precedente. Le liste possono essere ritirate fino al 20 aprile, e entro il 1 giugno l'autorita elettorale deve decidere se le liste e le eventuali richieste di ritiro sono accettate.

Voto

Il sistema Norvegese prevede diverse possibilità per esprimere il proprio voto, tra cui un periodo di early voting (dal 1 luglio al 9 agosto), uno di advance voting (dal 10 agosto al 9 settembre), voto dall'estero (tramite ambasciata dal 1 luglio al 2 settembre, o tramite posta in quei luoghi in cui non è presente un'ambasciata norvegese) oppure tramite internet nel periodo di advance voting per gli elettori delle le dieci municipalità selezionate per l'esperimento, sia dall'estero che all'interno della Norvegia.

Durante il periodo di early voting gli elettori possono organizzarsi per votare notificando le autorità municipali. A chi sceglie di votare in questo periodo viene data una scheda elettorale nazionale unificata, dato che le schede dei partiti non sono ancora state stampate (in Norvegia ogni partito ha una diversa scheda elettorale), e quindi non è possibile specificare nessuna preferenza per i candidati.

Durante l'advance voting vengono aperti diversi punti di voto in ospedali, università, scuole, prigioni e altri luoghi come librerie e centri commerciali. Alcuni di questi punti sono aperti per tutto il periodo, altri solo uno o più giorni. Chi sceglie di votare durante l'advance voting può farlo in qualsiasi circoscrizione elettorale, e nel caso un elettore decida di votare in una circoscrizione in cui non è registrato deve usare una scheda nazionale unificata come quella per l'early voting. Le schede di chi ha votato in una municipalità diversa da quella in cui risiede saranno poi mandate a quella di competenza.

Anche chi vota dall'estero tramite ambasciata o posta utilizza la scheda unificata, e il voto deve essere fatto entro il 4 settembre.

Le schede dell'advanced voting vengono messe sotto chiave negli uffici municipali ogni notte. Inoltre vengono periodicamente raccolte dai vari punti

dalle autorità municipali, ognuna poi viene mandata alla municipalità dell'elettore e vengono confrontate con la lista degli elettori prima del giorno dell'elezione. I nomi di chi ha già votato nel periodo di advance voting vengono contrassegnati nella lista degli elettori in modo che non possano rivotare. Dopo il voto nel giorno dell'elezione, la lista di chi ha votato durante l'advance voting è confrontata con la lista finale degli elettori, per avere ulteriore conferma che nessuno abbia votato due volte.

Per votare nel giorno dell'elezione, un elettore entra nella cabina elettorale di un seggio, sceglie la scheda di un partito, se vuole esprime un voto preferenziale, e piega la scheda. Dopodichè mostra un documento di identificazione con foto agli ufficiali del seggio, se l'identificazione avviene correttamente e l'elettore è presente sulla lista degli elettori viene timbrata la scheda e messa nell'urna. Per votare tramite internet, un elettore (registrato nelle dieci municipalità che aderiscono all'esperimento) apre la pagina web www.evalg.stat.no, e si autentica tramite username e password che sono usati anche per altri servizi web del governo. Una volta autenticato correttamente viene inviato al suo cellulare un codice PIN da inserire, e una volta fatto viene visualizzata la scheda di voto elettronica, sulla quale l'elettore sceglie una lista di candidati (oppure ha l'opzione di dare un voto bianco). Una volta effettuata la scelta la scheda elettronica viene cifrata e firmata con la firma digitale dell'elettore (il sistema assegna una firma digitale a ogni elettore abilitato a poter votare tramite internet, dato che nei documenti personali non è presente in Norvegia). Gli elettori ricevono delle tessere elettorali con sopra stampati dei "return codes", che permettono di verificare che il proprio voto è stato correttamente immagazzinato nell'urna elettronica. Una volta immagazzinato il voto cifrato, una funzione matematica permette di calcolare i return codes senza decifrarlo. I codici vengono mandati tramite SMS all'elettore che può quindi confrontarli con quelli presenti nella sua tessera elettorale (che sono unici). Ogni elettore può rivotare tramite internet quante volte desidera.

Conteggio

Per garantire la segretezza della chiave necessaria per decifrare i voti elettronici viene formata l'Electoral Board, composta da 10 membri, ognuno rappresentante di un diverso partito, e a ciascuno di essi viene data una parte della chiave segreta. Il giorno dopo la chiusura dell'internet voting i voti elettronici vengono prelevati dal server in cui si trovano e inizia il Cleansing Process. Durante questo procedimento vengono separati gli ID dai singoli voti elettronici, subito dopo aver scartato voti multipli dello stesso elettore (mantenendo il più recente), voti di elettori che hanno votato anche su carta (il voto su carta ha sempre precedenza su quello elettronico), e voti di persone non presenti nella lista degli elettori. I voti vengono poi mischiati per rimuovere qualsiasi possibilità di risalire all'identità del votante.

Il giorno dell'elezione l'Electoral Board si riunisce e ricompone la chiave segreta per la prima volta, e subito dopo la chiusura dei seggi i voti elettronici vengono decifrati e contati. Vengono stabiliti i risultati e resi pubblici nel sistema di amministrazione elettorale online.

Il conteggio per i voti cartacei avviene come segue: il Polling Commitee di ogni seggio conta il numero di nomi contrassegnati nella lista degli elettori e verifica che il numero sia uguale al totale delle schede elettorali utilizzate e presenti nell'urna, e successivamente contano il numero di schede per ogni partito (ogni partito ha la sua scheda elettorale). Viene firmato un documento ufficiale coi risultati di questi conteggi e viene mandato, insieme a tutto il materiale elettorale, a livello municipale dove l'EC conta nuovamente tutte le schede. Questo conteggio, tranne che nei comuni più piccoli, viene effettuato tramite scanner che registra anche la preferenza espressa in ogni scheda. Le schede e tutto il resto del materiale vengono poi mandati al CEC, che è responsabile di determinare il risultato dell'elezione in base ai risultati provenienti dai singoli comuni. Viene effettuato un conteggio per stabilire i voti per candidato e stabilire così il risultato finale.

Considerazioni

Il processo di voto norvegese, soprattutto per quanto riguarda la parte elettronica, ha caratteristiche interessanti. La segretezza e l'integrità del voto sono rispettate, ci sono meccanismi per impedire voti multipli sia nei periodi early e advance che nel giorno dell'elezione, l'autenticazione tramite username e password e successivo PIN inviato al cellulare sembra abbastanza robusta, ma la cosa più interessante è la possibilità di poter rivotare più volte tramite internet e, eventualmente, di votare anche tramite scheda cartacea.

In questo modo si contrasta il vote buying, infatti un eventuale interessato a comprare il voto di un elettore non potrà avere la certezza che in un secondo momento l'elettore non riesprima la sua preferenza, tramite internet o al seggio. Poter votare anche al seggio inoltre da una sicurezza in più all'elettore, nel caso in cui abbia dubbi o timori riguardo ad un eventuale furto delle proprie credenziali di accesso. Per il voto familiare le considerazioni sono analoghe.

2.2.2 Olanda

L'elezione per il parlamento olandese del 2006 [8] ha visto l'impiego di entrambi i principali tipi di voto elettronico: tramite internet per chi si trovava all'estero e tramite macchina DRE in alcuni seggi. La scelta tra macchina DRE e scheda cartacea è stata lasciata a ogni comune, e anche all'interno dello stesso diversi seggi potevano avere un diverso metodo di voto.

Di seguito è illustrato il processo elettorale dell'elezione.

Organi

La struttura per le elezioni in Olanda fornisce diversi livelli di amministrazione: MoIKR, l'Electoral Council, il Credentials Committee of the House, Committees dei 19 distretti elettorali (Principal Electoral Committees), il sindaco, i consigli elettorali municipali, e la commissione del seggio. Il siste-

ma per la gestione delle elezioni è decentralizzato, lasciando alla discrezione delle amministrazioni locali la scelta di come condurre le elezioni nella loro municipalità. C'è quindi una certa varietà anche grazie alla possibilità di fare esperimenti legati al processo di voto permessi dalla legge.

MoIKR. il MoIKR sorveglia a livello nazionale la conduzione delle elezioni. Stabilisce eventuali regolamentazioni per gli esperimenti permessi dalla legge, come il voto tramite internet per i residenti all'estero. Sorveglia anche la scelta degli standard per tutte le macchine di voto elettronico, il loro test, la loro certificazione, e la divulgazione di regole per il loro uso. Il MoIKR ha anche l'autorità per nominare i 19 PEC per i 19 distretti elettorali, oltre ai 458 sindaci.

Municipal Electoral Committee. il Municipal Electoral Commitee, uno per ogni Comune, ha il compito di amministrare le elezioni localmente, sia quelle locali che nazionali, di mantenere a livello municipale un registro degli elettori computerizzato, e di mandare a ogni elettore registrato una voter registration card via posta, che l'elettore dovrà mostrare al seggio per poter votare. Decidono anche il metodo utilizzato per votare nelle polling station (carta o DRE) e la loro posizione. Gli esecutivi municipali nominano i membri di ogni comitato elettorale di seggio, che consiste in un presidente e due membri, con relativi sostituti. Spesso lo staff dei seggi è formato da impiegati pubblici che lavorano per il comune e che ricevono un addestramento adeguato prima di ogni elezione.

Principal Electoral Committee. i Principal Electoral Commitees (PECs) sono 19, uno per ogni distretto, e sono formati da 5 membri più 3 sostituti. Il sindaco del maggiore Comune del distretto è il presidente del PEC, e i membri sono nominati dal MoIKR che ha il potere di nomina e scioglimento. Ogni PEC si occupa della registrazione delle liste di candidati nel distretto di cui si occupa.

Electoral Council. l'Electoral Council (EC) un organo elettorale centrale, con sede a L'Aia. E' composto da 7 membri esperti nominati dal governo che servono per un periodo che può andare fino a 12 anni. Agisce come un organo di consulenza per le elezioni per il governo e parlamento, e può fornire consigli ai comuni e partiti. L'EC numera le liste di candidati. Riceve il protocollo (documento ufficiale riguardante l'elezione) da ognuno dei distretti elettorali, e entro 5 giorni dall'elezione comunica i risultati. (i protocolli non vengono resi pubblici).

Parliamentary Committee of Credentials. il Parliamentary Committee of Credentials (CC) è formato da 3 parlamentari nominati dalla House e si occupa della certificazione di coloro eletti alla House o al Parlamento Europeo. Controlla i protocolli dei 19 distretti e delle 10000 polling station per controllare accuratezza e completezza, e verifica le qualifiche di coloro eletti contro requisiti costituzionali e legali, inclusi età e nazionalità. Eventualmente può raccomandare al parlamento di ricontare i voti, o di ripetere il voto.

Registrazioni

Il sistema di registrazione degli elettori è automatico e passivo. Il registro degli elettori viene mantenuto dal Municipal Electoral Committee. Gli elettori all'estero che desiderano utilizzare l'internet voting devono fare richiesta per la registrazione non più tardi di quattro settimane prima dell'elezione.

Il PEC registra le liste di candidati per il distretto, ognuna delle quali deve essere supportata da firme di almeno 30 elettori che risiedono nel distretto stesso. I partiti già rappresentati in parlamento non necessitano delle firme di supporto, e se concorrono con la stessa lista in tutti i distretti possono registrarla centralmente tramite l'Electoral Council.

Voto

Nell'elezione del 2006 sono state usate due distinte tecnologie di voto elettronico: macchine DRE nei seggi elettorali che ne prevedevano l'utilizzo e voto tramite internet per gli elettori all'estero che si sono registrati per utilizzarlo.

Per votare tramite DRE, un elettore tocca il punto sulla superficie della macchina etichettato col nome di un certo candidato, e questo viene interpretato dalla macchina come un tentativo di voto per quel candidato. La superficie è un touschscreen coperto dall'immagine di una scheda elettorale, con la rappresentazione dei partiti e dei candidati. Per confermare la scelta di voto, che viene mostrata in uno schermo più piccolo, l'elettore preme un grande bottone rosso, e a quel punto il voto viene incorporato nei risultati. Alla chiusura dell'elezione, la macchina stampa il totale dei voti tramite una piccola stampante interna, e quello diventa la documentazione ufficiale dei risultati riguardante quel seggio elettorale. Dall'istante in cui la votazione viene effettuata fino a quando il documento è stampato, i voti esistono soltanto in forma elettronica all'interno della macchina.

Come alternativa al voto tramite posta per gli elettori all'estero, il governo ha deciso di utilizzare un sistema di internet voting chiamato RIES (Rijnland Internet Election System) [12]. Chi si trova all'estero e desidera utilizzare questo sistema deve registrare la propria richiesta non più tardi di quattro settimane prima dell'elezione. Dopodichè riceve per posta un libretto con le istruzioni e un codice di autorizzazione sigillato. Il libretto indirizza l'elettore verso il sito web del RIES, dove viene usato il codice di autorizzazione per votare, il tutto entro 4 giorni dall'elezione. Dopo aver votato, l'elettore riceve un "technical vote", così da poter verificare sul web, dopo la chiusura dei seggi, che il proprio voto sia stato conteggiato. Questo technical vote non svela per chi ha votato l'elettore, ma può essere decodificato dallo stato per rivelare il voto. Dopo la chiusura dei seggi, il cifrario che associa i technical votes ai nomi dei candidati viene pubblicato, insieme a tutti i technical votes ricevuti. Così chiunque voglia può scaricare e contare i voti.

Ci sono quindi due procedure separate, una per gli elettori in Olanda e una per quelli all'estero. Gli elettori in Olanda si devono recare al seggio e devono mostrare e consegnare la tessera elettorale (voter card) ricevuta per posta per poter votare, sia che nel seggio si utilizzi il voto su carta che con macchina DRE. Gli elettori all'estero sono registrati al comune de L'Aia e votano tramite posta o internet in base alla scelta fatta alla registrazione. I circa 10000 seggi elettorali sono aperti dalle 7:30 alle 21:00. Gli elettori possono votare in un qualsiasi seggio nel proprio comune.

Una caratteristica particolare del processo elettorale olandese è il cosiddetto voto proxy. Il proxy vote da a un elettore che non è in condizione di potersi recare al seggio (ad esempio chi si trova in prigione) la possibilità di affidare il proprio voto a un altro elettore di sua fiducia. Per poter effettuare un proxy voting, il delegato deve portare al seggio la voter registration card dell'elettore per cui vota firmata, e deve votare a sua volta. Inoltre la voter registration card del delegato deve essere firmata sia da lui che dall'elettore per cui vota. Ogni elettore può effettuare al massimo due voti proxy.

Conteggio

Dopo l'elezione, ogni seggio con una DRE stampa dalla macchina i risultati. La stampa mostra il numero dei voti ottenuti da ciascuna lista, i voti per ogni candidato e il numero di voti bianchi. Il documento ufficiale contiene anche altri dati quali il numero di voter card raccolte e il numero di voti proxy. Il numero totale delle voter card raccolte deve essere uguale al numero totale di voti registrato dalla macchina DRE. Il presidente del seggio porta il documento ufficiale e il materiale di voto rimanente al Municipal Electoral Commitee. Le cartucce di memoria delle macchine sono portate insieme a quel materiale oppure vengono raccolte da impiegati municipali. Le cartucce, una volta arrivate agli uffici del comune, vengono lette da un computer e viene fatta una tabulazione automatica. Nel caso la memoria della macchina fosse illeggibile, vengono immessi manualmente i risultati riportati nel foglio

stampato. In aggiunta, i risultati tabulati vengono confrontati con i risultati stampati di tutti i seggi del comune.

Nei seggi in cui si vota tramite carta il conteggio e la tabulazione sono fatti in maniera simile, ma che richiede ovviamente più tempo. I voti vengono ordinati per liste, e vengono contati quelli per ogni lista (quelli invalidi e bianchi sono contati separatamente), dopodiché per ogni lista vengono divisi per candidato e contati, e i totali vengono riportati nel documento ufficiale.

Ogni Comune presenta i dettagli dei voti al PEC del proprio distretto, che determina i voti per ogni candidato e il totale per ogni partito, e comunica i risultati alle 10:00 a un incontro pubblico il secondo giorno dopo l'elezione.

Un rapporto ufficiale viene mandato lo stesso giorno all'Electoral Council. Tre giorni dopo l'EC stabilisce i risultati dell'elezione in base ai documenti ufficiali arrivati dai PECs.

Considerazioni

In Olanda il voto elettronico non è più utilizzato dal 2006, a causa di uno scandalo sollevato da un gruppo di persone in cui si dimostrava che le macchine DRE potevano essere manipolate con relativa facilità [13]. Rimane comunque utile poter valutare il processo di voto nella sua interezza, in modo da verificare se le potenziali vulnerabilità sono limitate alle macchine.

La particolarità del processo olandese è l'utilizzo di entrambe le principali tecnologie di voto elettronico, DRE in alcuni seggi e internet voting per chi si trova all'estero e lo desidera. Ogni elettore, quando si reca al seggio per votare deve consegnare la tessera elettorale ricevuta per posta, e questo impedisce che si verifichino casi di voti multipli da parte dello stesso elettore. Chi vota dall'estero, invece, deve fare richiesta di registrazione specificando la modalità desiderata di voto, quindi anche in questo caso non è possibile votare più volte. L'utilizzo di macchine DRE nei seggi, oltre ad aumentare l'accessibilità al voto, permette di avere un conteggio automatico dei voti.

Questo è utilizzato come confronto al conteggio manuale effettuato dagli operatori del seggio, in modo da limitare eventuali errori umani.

2.2.3 Estonia

L'elezione del 2007 in Estonia [7] è uno dei più famosi casi europei riguardanti l'internet voting [15, 1]. In questo caso il voto elettronico era disponibile per chiunque, e faceva affidamento a un forte sistema di identificazione nazionale.

Organi

La sistema elettorale estone fa affidamento su una struttura amministrativa a tre strati, responsabile della preparazione e conduzione dell'elezione.

NEC. è un organo con 7 membri nominati per un periodo di 4 anni. Le responsabilità del NEC includono il diritto di sospendere azioni delle commissioni di piu basso livello, sospendere membri di tali commissioni che violano il Riigikogu Election Act o le direttive del NEC o di una commissione a loro superiore. Il NEC da direttive per le nomine e registrazione dei candidati, per il voto, per la verifica dei risultati e per il conteggio. E' inoltre responsabile per la gestione del voto tramite internet.

CEC. Ci sono 17 CEC (uno per contea e altri due per due città, Tallin e Tartu), formati da 13 membri ognuno e nominati per un periodo di 4 anni. Ogni CEC è responsabile di istruire e supervisionare i DC e le loro attività, e anche della tabulazione e verifica dei risultati della votazione nella contea/città.

DC. i DC, composti da un presidente e altri membri fino a un massimo di 8, sono responsabili dell'amministrazione delle elezioni a livello dei seggi. I DC, al contrario degli organi di più alto livello, sono temporanei. Vengono nominati entro 20 giorni prima dell'elezione.

Registrazioni

La preparazione della lista degli elettori è organizzata tramite il registro della popolazione. Venti giorni prima dell'elezione vengono mandate delle tessere elettorali agli elettori in Estonia, che indicano i loro dati personali presi dal registro e il comune e il numero di seggio in cui sono inclusi nella lista degli elettori, e il luogo in cui si trova. La lista degli elettori deve essere consegnata a tutte le commissioni di seggio entro 7 giorni prima dell'elezione, quando inizia l'advance voting in tutti i seggi.

Voto

La base del sistema di internet voting in Estonia è l'utilizzo di un documento di identificazione personale (ID card), un documento obbligatorio che è accettato legalmente per l'identificazione tramite internet e per firmare digitalmente documenti. Gli elettori con una ID card abilitata possono votare tramite internet durante il periodo di advance voting, che va da 6 a 4 giorni prima del giorno dell'elezione. La legge permette anche di cambiare il proprio voto durante quel periodo, votando ancora tramite internet oppure attraverso sistema cartaceo nei seggi. Da notare che al voto cartaceo viene data più priorità, quindi in caso di voto elettronico e cartaceo viene considerato soltanto il cartaceo indipendentemente da quale è avvenuto prima.

Per votare tramite internet il computer utilizzato dall'elettore deve avere un lettore di smart card (facilmente acquistabile per un costo di circa 20 Euro) per poter leggere l'ID card. L'elettore deve accedere alla Voting Application (per gli utenti Windows si accede ad essa collegandosi al sito www.valimised.ee, per Mac OS e Linux è un programma a sé stante), la quale richiederà i dati della sua ID card che dovrà quindi essere inserita nel lettore. Per procedere, l'elettore deve digitare un codice personale (PIN1, è uno dei due PIN che sono associati alla sua ID card). L'applicazione controlla se l'elettore è nella lista degli elettori, in caso di esito negativo viene comunicato all'utente di contattare la Population Registration Authority, in caso

di esito positivo l'applicazione mostra la lista dei candidati per ogni partito in base al distretto elettorale dell'elettore. L'elettore sceglie un candidato da una lista di partito o un candidato indipendente clickando sul nome e poi conferma la sua scelta. Il voto viene cifrato con la chiave pubblica del Counting Server, e l'utente deve digitare il suo secondo codice personale (PIN2) per poter effettivamente dare il proprio voto. Il codice permette alla ID card di firmare il voto cifrato. Il voto viene mandato all'Internet Server dove viene controllato se la firma corrisponde al proprietario della sessione (cioè se chi ha votato è la stessa persona che ha iniziato il processo). L'Internet Server poi, in caso positivo, manda il voto cifrato al Vote Storage Server, che richiede un controllo sulla validità del certificato dell'elettore dal Certificate Server. Se valido, l'Internet Server verifica la firma digitale usando la chiave pubblica dell'elettore dal certificato dell'elettore. Alla fine del processo di voto l'elettore riceve su monitor una conferma del fatto che il voto è stato dato. Il voto resta nel Vote Storage Server fino al momento del conteggio e tabulazione il giorno dell'elezione.

Conteggio

Il NEC fornisce ai CECs una lista per ogni seggio che contiene i nomi degli elettori che hanno votato tramite internet. I DCs marcano nella loro lista degli elettori coloro che compaiono nella lista fornita dal NEC. Chi ha votato tramite internet non può votare il giorno dell'elezione. Dopo aver ricevuto dai seggi le liste riguardanti gli elettori che hanno votato tramite scheda cartacea durante l'advance voting, il NEC marca i voti internet di quegli elettori (se presenti) come da non contare, dopodichè viene messo su CD l'ultimo voto elettronico di ogni elettore e il CD viene consegnato al presidente del NEC. Un'ora dopo la chiusura dei seggi, nel giorno dell'elezione, inizia il conteggio dei voti elettronici. I voti sono messi da CD sul Counting Server, il quale li decifra e li conta. I voti sono decifrati dal server usando l'Hardware Security Module (HSM), per abilitare il quale sono necessarie 6 chiavi fisiche, 2 sono in

possesso degli operatori e altre 7 sono in possesso del NEC, ogni membro ne ha una, quindi per contare i voti devono essere presenti almeno 4 membri del NEC, presidente incluso. Una volta contati i voti, vengono messi i risultati su un altro CD e caricati su un personal computer in modo da poter essere visti in un foglio elettronico.

Considerazioni

Il processo di voto estone è un esempio classico in letteratura quando si parla di e-voting. Il processo è ben studiato, e riesce a integrare bene il voto elettronico con il voto cartaceo: chi vota tramite internet non può votare al seggio il giorno dell'elezione, e chi ha votato durante l'advance voting vedrà un suo eventuale voto tramite internet non conteggiato. Tutto questo serve a impedire voti multipli da parte di uno stesso elettore. La segretezza del voto tramite internet viene garantita tramite cifratura, e l'autenticazione basata su ID card nazionale rende il processo abbastanza sicuro.

2.2.4 Svizzera

L'organizzazione e l'amministrazione delle elezioni federali in Svizzera varia molto da un cantone all'altro e da un comune all'altro [3, 11], ed è quindi possibile solo riportare una panoramica generale dell'elezione del 2011 [10].

Organi

Federal Chancellery. Ha ruolo di coordinazione per le elezioni federali ed è responsabile per quanto riguarda il rispetto delle regole e degli standard. Fornisce informazioni ai partiti riguardo la registrazione dei candidati e controlla la loro idoneità, sovrintende l'uso dell'internet voting e pubblica i risultati finali.

Canton. Le procedure amministrative legate alle elezioni vengono svolte, a livello di cantone, da impiegati civili del cantone. Ogni cantone è

responsabile della preparazione delle schede elettorali e delega il resto delle responsabilità ai singoli comuni.

Comune. Ogni comune è responsabile dell'invio agli elettori delle schede elettorali, dell'amministrazione dell'early voting, delle operazioni che si svolgono ai seggi e del conteggio.

Registrazioni

Il sistema di registrazione degli elettori è un sistema passivo. Ogni comune mantiene un registro della popolazione aggiornato dal quale viene estratto il registro degli elettori. Il tutto è efficiente e assicura che un elettore che cambia comune di residenza venga tolto dal registro del vecchio comune e inserito in quello del nuovo. I cambiamenti al registro possono essere fatti entro 5 giorni prima dell'elezione. I cittadini svizzeri all'estero possono registrarsi all'ambiasciata più vicina, che inoltra i dettagli della registrazione al comune interessato.

In generale, i partiti sottopongono alla cancelleria di un cantone una lista con a supporto un certo numero (da 100 a 400, dipende da ogni cantone) di firme di elettori aventi diritto al voto di quel cantone. Le firme non sono necessarie se il partito è rappresentato nel Consiglio Nazionale, e se propone una sola lista di candidati nel cantone oppure se alle precedenti elezioni ha ottenuto almeno il 3

Voto

Prima di tutto è necessario specificare che il sistema di voto svizzero è molto complesso. A ogni elettore viene spedito un pacchetto contenente una scheda separata per ogni lista di candidati, e in aggiunta una scheda bianca. Agli elettori è consentito un numero di voti pari al numero di seggi che il cantone ha nel National Council. Il voto offre diverse opzioni agli elettori:

- Votare per una lista di candidati nella sua interezza.

- Votare per una lista di candidati, cancellando alcuni nomi e aggiungendone altri da altre liste.
- Votare utilizzando la scheda bianca scrivendo qualsiasi combinazione di nomi di candidati da qualsiasi lista, fino al numero di seggi del cantone nel National Council.
- Votare scrivendo il nome di una lista in alto nella scheda bianca, e inserendo nomi di candidati da qualsiasi lista. Eventuali spazi vuoti sono assegnati alla lista scritta in cima.

In svizzera sono consentite diverse forme di voto. Il voto per posta è possibile per chiunque, anche per i residenti all'interno della nazione, e è molto sfruttato. Le autorità di ogni cantone si occupano di preparare il materiale di voto e agli elettori almeno dieci giorni prima dell'elezione (per gli elettori all'estero il materiale elettorale si invia una settimana prima che per chi si trova in Svizzera). Il materiale inviato comprende tessera e scheda elettorali, busta in cui mettere tessera e scheda una volta espresso il voto (o più di una in caso di più schede elettorali se si deve esprimere più di un voto) e informazioni sui partiti. Una volta ricevute le buste, lo staff del comune le controlla per verificare eventuali invalidità: mancanza di tessera elettorale, mancanza di firma dell'elettore, o in alcuni cantoni omissione della data di nascita. In genere si cerca di evitare schede invalide, e in alcuni cantoni o comuni viene contattato l'elettore se, ad esempio, manca la firma, e viene invitato a presentarsi per rimediare. Dal momento che la responsabilità per l'organizzazione e amministrazione dell'elezione ricade sui singoli comuni, il voto nei seggi è gestito in molti modi diversi. Generalmente un membro dello staff del seggio si occupa di ricevere dagli elettori le tessere elettorali, che in alcuni cantoni deve essere firmata. Nella maggior parte dei cantoni non c'è nessun controllo sull'identità del votante. Una volta espressa la propria preferenza sulla scheda elettorale, l'elettore la fa timbrare sul retro a un apposito membro dello staff, dopodiché viene messa nell'urna. Alcuni cantoni,

comuni, o seggi hanno utilizzato procedure migliori, come ad esempio mettere la scheda elettorale dentro una busta prima di farla timbrare o avere un registro degli elettori per verificare l'identità. L'internet voting è permesso solo ai cittadini dei quattro cantoni aderenti all'esperimento (Aargau, Basel-Stadt, Graubünden, St. Gallen) che vivono all'estero. Sono stati usati due sistemi: il "Geneva system" nel cantone di Basel-Stadt e il "consortium system" nei rimanenti. L'identificazione dell'elettore avviene tramite la tessera elettorale che gli è stata spedita, e contiene un numero di identificazione unico e credenziali di voto, ossia un codice di identificazione e una password. Il codice di identificazione serve per aprire una scheda, e la password per inviare il voto. Entrambi i sistemi non permettono all'elettore di esprimere un voto invalido, o di cambiarlo dopo che è stato inviato. Inoltre manca un meccanismo che permetta a chi ha votato di vedere se il suo voto è stato registrato correttamente. Una volta inviato il voto, la scheda viene depositata in un'urna elettronica. Qui i due sistemi si differenziano: il consortium system cifra il voto solo una volta ricevuto dal server, mentre il Geneva system lo cifra nel computer dell'elettore prima dell'invio.

Conteggio

Anche nel conteggio le procedure usate dai diversi cantoni sono differenti. In generale alla chiusura dei seggi il presidente del seggio conta il numero di tessere elettorali raccolte per vedere quanti hanno votato, e insieme all'urna vengono portate a livello comunale o cantonale per il conteggio. Le schede per il National Council sono separate in schede che non hanno subito cambiamenti e schede in cui gli elettori hanno cancellato o scritto nomi. Le prime sono introdotte direttamente nel sistema come blocco di voti per il partito a cui fanno riferimento, le altre vengono controllate attentamente per verificare che non siano invalide, e vengono poi contate individualmente per candidato. Finito il conteggio vengono utilizzate per inserire i dati che contengono in un sistema di tabulazione elettronico.

Considerazioni

Il processo di voto svizzero è difficile da analizzare in quanto non è uniforme nei vari cantoni e/o comuni. La mancanza di forti norme comuni e di procedure che sarebbe utile adottare (come la verifica dell'identità dell'elettore in tutti i seggi, o mettere la scheda elettorale in una busta prima di farla timbrare in modo da assicurare la segretezza del voto) rende l'intero processo basato più che altro sul senso civico e sulla fiducia degli elettori. Anche il sistema di voto elettronico ha difetti, come un'autenticazione debole (basata su informazioni stampate sulla tessera elettorale spedita per posta) e l'impossibilità di verificare la corretta registrazione del voto.

Capitolo 3

Strumenti di analisi

In questo capitolo vengono presentati gli strumenti di modellazione e analisi utilizzati in [17, 18, 16, 19] per rappresentare un processo elettorale ed analizzarlo in cerca di vulnerabilità, con lo scopo di proporne miglioramenti. Gli strumenti di questo capitolo verranno poi utilizzati nel capitolo 4 per modellare e analizzare uno dei processi elettorali del capitolo 2.

3.1 Little-JIL

Little-JIL [4] è un linguaggio visuale di coordinazione di agenti. I programmi in Little-JIL descrivono l'ordine e la comunicazione tra unità di lavoro chiamate step. Assegnando gli step a degli agenti, il programma assiste gli agenti nel completamento del processo.

Un agente è un'entità autonoma esperta in una certa parte del processo descritto dal programma in Little-JIL. Un agente può essere una persona, un gruppo di persone, un componente hardware o un sistema software.

Uno step è la definizione di una unità di lavoro che viene assegnata a un agente. Ogni step può contenere specifiche su informazioni e risorse necessarie, prerequisiti che devono essere soddisfatti prima che l'agente inizi il lavoro, e postrequisiti per controllare che il lavoro sia stato svolto corretta-

mente. Uno step specifica anche in che modo dovrebbe reagire ad eventi o errori che possono avvenire durante la sua esecuzione. Una definizione di processo in Little-JIL si compone di tre parti principali:

- Un diagramma di coordinazione: è la rappresentazione grafica del processo, formato da step. Ogni step può essere decomposto in substep, fino ad avere le unità di lavoro più elementari (step foglia).

- Un artifact model: è l'insieme dei tipi di dato che sono usati dagli oggetti passati tra i vari step durante l'esecuzione del processo. Per definire i tipi di dato viene usato Java.

- Resource model: descrive le risorse condivise dagli agenti durante l'esecuzione del processo. Anche gli agenti sono associati agli step come risorsa.

Di seguito è fornita una presentazione del linguaggio, del quale [21, 22] contengono una guida iniziale.

3.1.1 Step

Uno step è l'unità di costruzione base per un programma in Little-JIL. Rappresenta un'unità di lavoro e può essere suddiviso in substep.

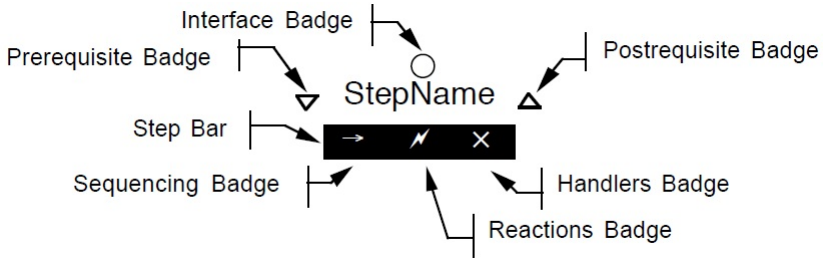

Figura 3.1 – *Icona rappresentante un generico step.*

Dopo la sua istanziazione, uno step in Little-JIL può trovarsi in sei stati:

- Posted: quando uno step è pronto a iniziare la sua esecuzione. Vengono verificate la disponibilità di eventuali risorse richieste, inizializzati i parametri, e viene assegnato un agente allo step.

- Started: uno step è started quando l'agente vuole iniziare il lavoro specificato dallo step. Vengono acquisite le risorse necessarie e controllati i pre-requisiti. Per uno step con substeps, started significa che i suoi substeps passano in stato posted (in base al sequencing badge).

- Completed: uno step completed è uno step il cui lavoro si è concluso con successo. Vengono controllati i post-requisiti e rilasciate le risorse. Uno step con substeps è completed quando i suoi substeps sono retracted, completed o terminated.

- Terminated: uno step terminated è uno step che non ha portato a termine con successo il proprio lavoro. Lo stato terminated può essere indotto da un'eccezione nello step o in suoi substeps, o dalla mancata disponibilità di risorse.

- Retracted; uno step retracted solitamente è uno substep non scelto di uno step choice.

- Opted out: solo per step opzionali. Uno step opted out è uno step il cui agente ha indicato che non sarà eseguito.

I substeps di uno step sono rappresentati sotto lo step padre e sono connessi ad esso tramite una linea che unisce la parte alta del substep e il sequencing badge dello step padre.

L'esecuzione dei substep di uno step padre può avvenire in diversi modi. Il sequencing badge del padre specifica esattamente l'ordine di esecuzione dei figli. Ci sono cinque diversi tipi di modalità di esecuzione specificate dal sequencing badge: nessuna, sequenziale, parallelo, choice, try.

Se il sequencing badge è vuoto, lo step non può avere substep (è uno step foglia) ed è eseguito interamente dall'agente assegnato ad esso.

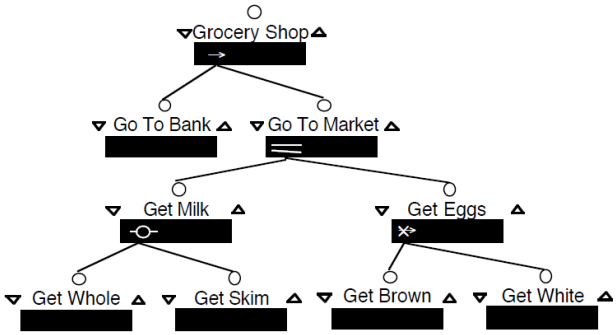

Figura 3.2 – *Esempio di gerarchia di step in una definizione di processo in Little-JIL.*

Figura 3.3 – *Icona rappresentante uno step foglia.*

Se il sequencing badge è una freccia, l'ordine di esecuzione dei substep è sequenziale. Uno step sequenziale esegue ognuno dei suoi substep in ordine da sinistra a destra, iniziandone uno quando il precedente è terminato. Uno step sequenziale termina quando tutti i suoi substep sono terminati.

Se il sequencing badge rappresenta due linee orizzontali, l'ordine di esecuzione dei substep è parallelo. I substep di uno step parallelo vengono eseguiti tutti concorrentemente, e una volta terminati tutti termina lo step padre.

Se il sequencing badge è un cerchio con una riga orizzontale, è uno step choice. Uno step choice permette di scegliere uno degli step figli da eseguire, e una volta terminato termina anche lo step choice. Eventuali handlers possono

Figura 3.4 – *Icona rappresentante uno step sequenziale.*

Figura 3.5 – *Icona rappresentante uno step parallelo.*

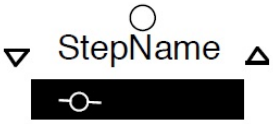

Figura 3.6 – *Icona rappresentante uno step choice.*

permettere una ulteriore scelta nel caso il substep fallisse l'esecuzione.

Figura 3.7 – *Icona rappresentante uno step try.*

Se il sequencing badge è una freccia con sopra una X, è uno step try. In uno step try si provano alternativamente i substep, da sinistra a destra, fino a quando uno di essi conclude l'esecuzione con successo. Una volta terminato con successo il substep termina anche lo step try.

3.1.2 Risorse

Una risorsa è un'entità per la quale c'è contesa per l'accesso. Il prodotto di uno step può essere una risorsa per un altro step. L'insieme delle risorse modellate in un processo è il resource model. Tutte le dichiarazioni di risorse hanno un modo e un nome. ci sono cinque modalità per la dichiarazione di una risorsa: acquisition, use, collection, collection iterator, collection use.

- Resource acquisition: questa modalità serve per dichiarare una risorsa che deve essere acquisita prima che lo step possa iniziare la sua esecuzione.
- Resource use: questa modalità dichiara una risorsa che sarà fornita da un altro step.
- Resource collection: una resource collection è un sottoinsieme (potenzialmente anche vuoto) del resource model. Può essere usata per rappresentare gruppi di risorse all'interno di un programma.
- Resource collection iterator: si tratta di una resource collection che condivide uno stato di iterazione tra tutti i suoi usi (vedere Carinalità).
- Resource collection use: questa modalità dichiara una resource collection che sarà fornita da un altro step.

Agenti come risorse

L'agente è un tipo speciale di risorsa per uno step in Little-JIL. Un agente può essere dichiarato come risorsa per lo step, altrimenti nel caso non fosse dichiarato viene ereditato l'agente dallo step padre. Ogni step deve avere un agente, quindi ogni programma rappresentante un processo in Little-JIL deve almeno dichiarare un agente per lo step root.

3.1.3 Parametri

Il passaggio di parametri è un meccanismo che può essere utilizzato per passare informazioni tra step padri e figli nella gerarchia di un programma in Little-JIL. Ogni step può avere dei parametri, ogni parametro ha un nome, un tipo, una modalità, e un valore di default (opzionale). Il nome è utilizzato per identificare il parametro e serve per eseguire il binding e comunicare con l'agente. Il tipo di un parametro è dichiarato esternamente a Little-JIL, viene utilizzato Java. Le modalità di un parametro sono le seguenti:

- In: i parametri in, rappresentati da una freccia che punta verso il basso, sono parametri il cui valore viene copiato nello step quando lo step è posted.

- Out: i parametri out, rappresentati da una freccia che punta verso l'alto, sono parametri il cui valore viene copiato verso l'esterno quando lo step completa la sua esecuzione.

- In/out: rappresentati da una doppia freccia verso l'alto e verso il basso, sono copiati in uno step quando è posted e vengono copiati verso l'esterno quando completa la sua esecuzione.

- Local: i parametri local sono creati all'interno di uno step per permettere la comunicazione tra i suoi substep. Questi parametri sono visibili soltanto ai substep dello step in cui sono dichiarati.

Passaggio di parametri

E' possibile passare i parametri tra gli step per mezzo del binding. Un binding associa una costante o un parametro in uno step con un parametro in un suo substep. Il binding di un parametro è rappresentato dalla notazione

parametro-substep freccia *parametro-step-padre*

La freccia indica la direzione del flusso dell'informazione, da o verso lo step padre, determinato dalla modalità del parametro del substep. Per il passaggio dei parametri è importante la loro compatibilità: due parametri sono compatibili se i loro tipi sono compatibili, e se le loro modalità permettono di copiare i valori nella direzione desiderata. La modalità in/out è compatibile con diverse altre modalità, ed è possibile avere binding separati per l'in e per l'out. Si può effettuare il binding di un parametro con una costante se la modalità del parametro è in o in/out.

3.1.4 Cardinalità

La cardinalità è un meccanismo per esprimere l'opzionalità di uno step o la sua ripetizione. Il numero di istanze di uno step che devono essere create può essere specificato staticamente, determinato dall'agente assegnato allo step, o può dipendere dalla disponibilità di artefatti o risorse. La cardinalità è rappresentata accanto al connettore che collega il substep a cui si riferisce al suo step padre, tramite le seguenti notazioni:

- ?: indica che lo step è opzionale.
- +: indica che lo step deve essere istanziato almeno una volta.
- *: indica che lo step deve essere eseguito zero o più volte.
- N: indica che lo step deve essere istanziato esattamente N volte.
- L..U: indica che lo step deve essere istanziato almeno L volte e al più U volte.
- N+: indica che lo step deve essere istanziato N o più volte.

Se la cardinalità non è un singolo bound statico (ad esempio 2, indicando che lo step deve essere istanziato 2 volte), la ripetizione dello step dovrà dipendere da una qualche decisione esterna. Se non viene specificato altro, l'agente assegnato allo step controlla l'esecuzione tramite la capacità di poter far andare lo step in stato opted out. L'agente può prendere quella decisione solo quando la cardinalità lo permette: con una cardinalità di 2..4, l'agente potrà effettuare quella scelta soltanto alle iterazioni 3 e 4.

Per uno step con sequencing badge sequenziale o try, dopo che l'istanza di uno step viene completata, viene creata un'altra istanza fino a quando viene raggiunto il limite superiore o l'agente decide di non eseguire altre istanze. Per step con sequencing badge parallelo o choice, vengono portate in posted abbastanza istanze per soddisfare il limite inferiore, e un'altra istanza viene

creata subito dopo lo starting di una di esse, fino a quando ne vengono create a sufficienza da soddisfare il limite superiore.

Il numero di istanze di uno step può essere controllato anche dal numero di risorse o artefatti disponibili. Il nome della risorsa o artefatto viene incluso nella cardinalità, e combinati con i bound statici visti in precedenza (per esempio, si può venire a creare un bound del tipo nomeparametro(2..4), oppure nomeparametro+). La cardinalità di default per un bound legato a risorse o artefatti è +, che significa utilizzare tutte le risorse o artefatti disponibili e richiede che ce ne sia almeno una. Per step sequenziali o try, a ogni istanza viene assegnata una risorsa o artefatto, e l'iterazione termina quando non ci sono più risorse disponibili. Il comportamento degli step paralleli è try è simile, con la differenza che tutte le istanze sono create quando lo step padre va in stato started.

E' possibile utilizzare un resource collection iterator per creare una iterazione su risorse condivisa da più step. In questo caso quando una risorsa viene assegnata a una istanza di step, non può essere acquisita da altri step che condividono il resource collection iterator.

Esiste un ulteriore modo per controllare l'istanziazione di substep: tramite predicati (o espressioni). Questo meccanismo condizionale permette di specificare un'espressione, in un linguaggio esterno a Little-JIL, che se valutata vera causa il posting dello step, altrimenti lo step padre prosegue come se il substep non fosse mai stato presente.

3.1.5 Requisiti

I requisiti forniscono un meccanismo per definire condizioni sull'entrata in e sull'uscita da step. Se un requisito fallisce, lancia un'eccezione che si propaga fino allo step padre, che può avere un handler per gestirla.

Un requisito è uno step che è referenziato dal pre- o post-requisite badge di un altro step, nel caso si tratti rispettivamente di requisito in entrata o in uscita.

E' possibile passare parametri a uno step requisito, ma non dovrebbe avere parametri di tipo out o in/out, in quanto lo scopo di un requisito non è avere effetti sull'elaborazione ma controllare condizioni.

Se un requisito fallisce la sua esecuzione, lancia un'eccezione e lo step a cui è associato termina. Eventualmente, è possibile utilizzare anche i predicati come requisiti associati a uno step.

3.1.6 Exceptions

Le eccezioni sono utilizzate per indicare che una risorsa o un parametro non sono disponibili, o per indicare che un agente non ha potuto completare uno step. Ogni step specifica le eccezioni che è possibile lanciare da esso. Come per i parametri, le eccezioni sono definite con un linguaggio esterno a Little-JIL (Java).

Per gestire le eccezioni si utilizzano gli handlers. Se uno step riceve un'eccezione e non ha un handler per gestirla, lo step termina e l'eccezione viene propagata allo step padre.

Gli handler vengono rappresentati in rosso, connessi all'handler badge dello step che gestisce l'eccezione.

3.2 Fault Tree Analysis

La Fault Tree Analysis (FTA) [6, 20, 18] è una tecnica analitica deduttiva top-down utilizzata in vari settori per studiare i rischi.

Con la FTA prima di tutto si formula un possibile rischio, e poi si cerca di scoprire quali eventi nel processo potrebbero combinarsi causando il verificarsi del pericolo.

3.2.1 Fault Tree

Dato il rischio, la FTA produce un fault tree, un modello grafico di tutte le varie combinazioni di eventi che potrebbero portare al pericolo.

Un fault tree consiste di due tipi di elementi: eventi e gates. Gli eventi sono rappresentati come rettangoli o ellissi, i gate tramite gate di logica Booleana. L'elemento più in alto nell'albero (root) è il pericolo. Nel fault tree gli eventi intermedi sono ulteriormente scomposti, mentre gli eventi primari no.

Gli eventi sono connessi l'un l'altro tramite gates di logica Booleana. Un gate collega due o più eventi input di più basso livello a un singolo evento outpu di più alto livello. Ci sono tre tipi di gate:

- AND: l'evento output si verifica se e solo se si verificano tutti gli eventi input, implicando che il verificarsi degli eventi di input causa l'evento output
- OR: l'evento output si verifica se e solo se almeno uno degli eventi input si verifica, implicando che il verificarsi di uno qualsiasi degli eventi input causa l'evento output.
- NOT: l'evento output si verifica se e solo se non si verifica l'unico evento input.

La figura 3.8 mostra un semplice esempio di fault tree con evento root, quindi il possibile rischio, *Artifact votingRoll from conduct election is wrong*. Un gate OR collega questo evento a un evento di più basso livello, *Artifact votingRoll is wrong when step count votes is completed*, mostrando che l'evento di più alto livello si verificherà se si verifica quello di più basso livello. L'evento *Artifact votingRoll is wrong when step count votes is completed* è a sua volta collegato a due eventi tramite un gate AND, il che significa che si verificherà solo al verificarsi di entrambi gli eventi a cui è collegato. Alla fine si arrivano ad avere eventi, come *Artifact votingPoll is wrong when step*

conduct election is posted, che non sono ulteriormente elaborati in quanto eventi primari.

Un fault tree può essere calcolato automaticamente dalla definizione di un processo in Little-JIL [5], e può essere utilizzato per determinare tutte le combinazioni di step eseguiti non correttamente che possono portare al verificarsi di un pericolo.

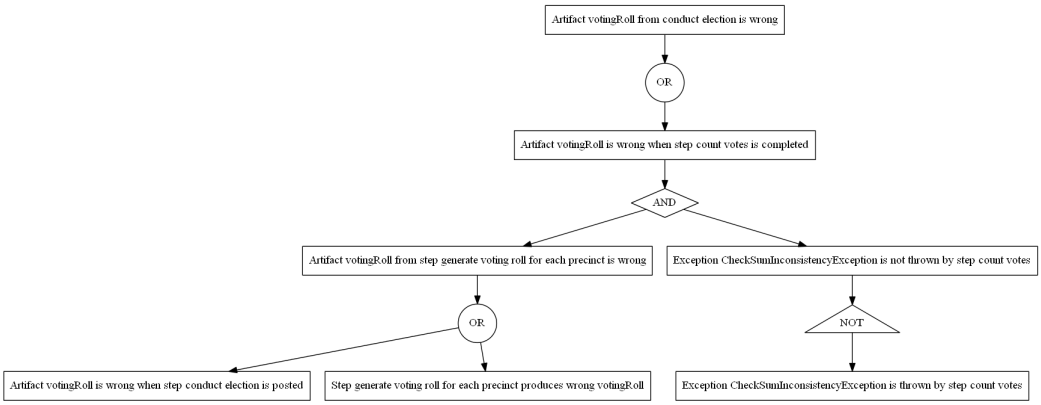

Figura 3.8 – *Un semplice fault tree.*

3.2.2 Minimal Cut Set

Un cut set è un insieme di eventi che causano il verificarsi del pericolo specificato in un fault tree. Un cut set è quindi formato da eventi primari o negazioni di eventi primari.

Un cut set è considerato minimo se, quando viene rimosso uno degli eventi che lo compongono, l'insieme risultante non è più un cut set.

Un minimal cut set (MCS) indica una potenziale vulnerabilità nel processo. Un MCS di grandezza 2 indica una combinazione di due eventi che insieme portano al verificarsi del pericolo. Un MCS con un solo elemento indica un single point of failure (SPF). I SPFs sono considerati le più pericolose sorgenti di vulnerabilità, in quanto indicano un singolo step nel processo che, quando eseguito non correttamente, porta al pericolo.

I MCS possono essere calcolati nel seguente modo: partendo dalla radice dell'albero viene costruita un'equazione Booleana per ogni gate, col nodo padre a sinistra e i nodi figli a destra. Se il gate è un OR i nodi figli sono connessi tramite l'operatore +, se è un AND tramite l'operatore *, in caso di NOT invece basta sostituire il nodo figlio con la sua negazione. Queste equazioni vengono risolte usando l'algebra Booleana standard, in cui 1 corrisponde a *true*, 0 a *false* e NOT converte 0 in 1 e viceversa. Se una clausola è composta di termini connessi tramite *, tutti i termini dovranno valere 1 perchè la clausola sia vera, se i termini sono connessi tramite + la clausola sarà vera se almeno uno di essi è 1.

Se uno dei nodi del lato destro dell'equazione è ulteriormente decomposto nel fault tree, allora viene sostituito dalla sua decomposizione nel modo descritto sopra. Le sostituzioni vengono eseguite fino a quando non sono più possibili, e si avrà un'equazione Booleana con il pericolo (il nodo root del fault tree) nella parte destra e solo eventi primari (i nodi foglia) nella parte sinistra. La parte destra viene trasformata in una rappresentazione più compatta grazie alle tecniche esistenti per la minimizzazione di espressioni Booleane, e trasformata in *disjunctive normal form* (una disgiunzione di clausole congiuntive).

Data l'equazione risultante, il pericolo si verificherà solo se una o più delle clausole congiuntive avrà valore *true*, ossia quando tutti i termini della clausola varranno *true*.

Quindi ogni clausola congiuntiva rappresenta un MCS.

Come per i fault trees, è possibile calcolare i MCS in modo automatico partendo da una definizione di processo in Little-JIL di cui si calcola il fault tree.

Capitolo 4

Caso di studio

In questo capitolo viene presentato come caso di studio il processo di voto utilizzato in Norvegia. Il processo è stato modellato utilizzando Visual-JIL, l'editor di Little-JIL costruito come componente per l'IDE Eclipse. Di seguito viene mostrato un esempio di applicazione di Fault Tree Analysis al processo norvegese, ossia la definizione di alcuni pericoli di interesse, i fault trees da essi derivati e i loro MCSes, e le interpretazioni di questi ultimi.

Lo scopo di questo caso di studio è verificare se gli strumenti di analisi presentati nel Capitolo 3, già utilizzati per modellare e analizzare il processo elettorale di Yolo County in California [18, 16], possono essere utilizzati più in generale per modellare e analizzare anche processi di altre parti del mondo e se il processo in esame, quello norvegese, presenta vulnerabilità degne di nota.

4.1 Metodologia

La metodologia utilizzata per l'analisi del processo di voto di Yolo County, California, si compone di due fasi: identificare potenziali attacchi ad un processo e analizzare la robustezza del processo in presenza di uno specifico attacco.

Nella prima fase viene utilizzato Little-JIL come linguaggio di modellazione di processo per modellare il processo reale. Si ipotizza che un individuo possa attaccare il processo, creando di conseguenza uno stato non desiderato. Si applica la Fault Tree Analysis al modello che è stato creato, specificando in modo formale il pericolo in modo da scoprire in quali circostanze tale pericolo potrebbe avvenire.

La Fault Tree Analysis produce un insieme di Minimal Cut Sets, ognuno dei quali contiene un insieme di eventi che, se verificati, causano il pericolo. I Minimal Cut Sets forniscono dettagli su come un attaccante potrebbe sfruttare le vulnerabilità del processo per creare il pericolo specificato.

4.2 Modello

In figura 4.1 viene presentato il modello del processo norvegese. Quella mostrata è la struttura generale del processo, nel modello completo alcuni step sono ulteriormente sviluppati (nello specifico, gli step senza triangoli ai lati del nome sono step *reference*, che fanno riferimento a step con lo stesso nome definiti in altri diagrammi).

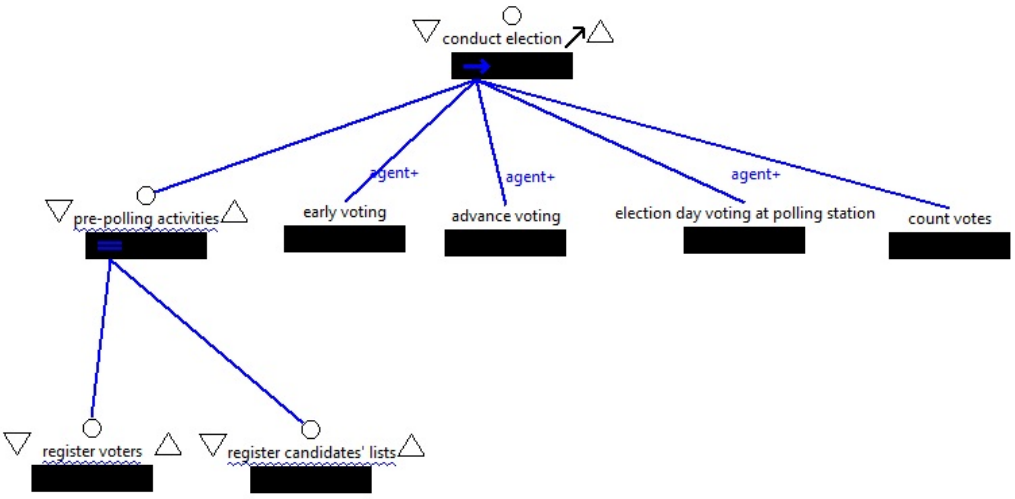

Figura 4.1 – *Il modello del processo di voto norvegese.*

Lo step root è *conduct election*, uno step sequenziale con cinque figli: *pre-polling activity*, *early voting*, *advance voting*, *election day at precinct*, *count votes*. Lo step sequenziale *pre-polling activity* ha due figli, *register voters* e *register candidates' lists*,e rappresenta le attività da svolgersi prima dell'inizio del voto vero e proprio, come appunto la registrazione degli elettori in un registro degli elettori e la registrazione delle liste di candidati. Lo step *early voting* è uno step reference, e rappresenta le attività svolte durante il periodo di early voting. Lo step *advance voting*, anch'esso reference, corrisponde alle attività del periodo di advance voting, ossia il voto dall'estero, il voto alle postazioni di advance voting nei vari comuni, e il voto tramite internet. Lo step *election day voting at polling station* è uno step reference che racchiude le attività da svolgersi il giorno dell'elezione vero e proprio in ognuno dei seggi. L'ultimo step, *count votes*, rappresenta la fase di conteggio dei voti.

Si può notare che nelle linee di collegamento tra lo step root e i suoi 3 step figli centrali appare la scritta *agent+*. Questa rappresenta il fatto che, per esempio, lo step *early voting* sarà eseguito una volta per ogni comune (l'agente responsabile dell'esecuzione dello step *early voting*). Stesso discorso per gli altri due step, con agenti rispettivamente comune e seggio.

Di seguito vengono presentati due diagrammi, quello relativo al voto nei seggi il giorno dell'elezione e quello relativo al voto tramite internet (che a sua volta è un substep dell'advance voting), che saranno poi utilizzati nella definizione di alcuni pericoli di esempio.

In figura 4.2 è rappresentato il modello del processo di voto nel giorno dell'elezione ai seggi. Lo step più in alto è lo stesso visto come step reference nel modello più generale. Qui si vede che è uno step sequenziale con quattro figli: *voting*, *authentication with photo ID*, *check off voter as voted* e *ballot in repository*.

Voting è uno step sequenziale nel quale viene modellato l'espressione del voto da parte dell'elettore, che prende una scheda relativa a un partito e la compila. Questa parte nel modello norvegese viene insolitamente prima,

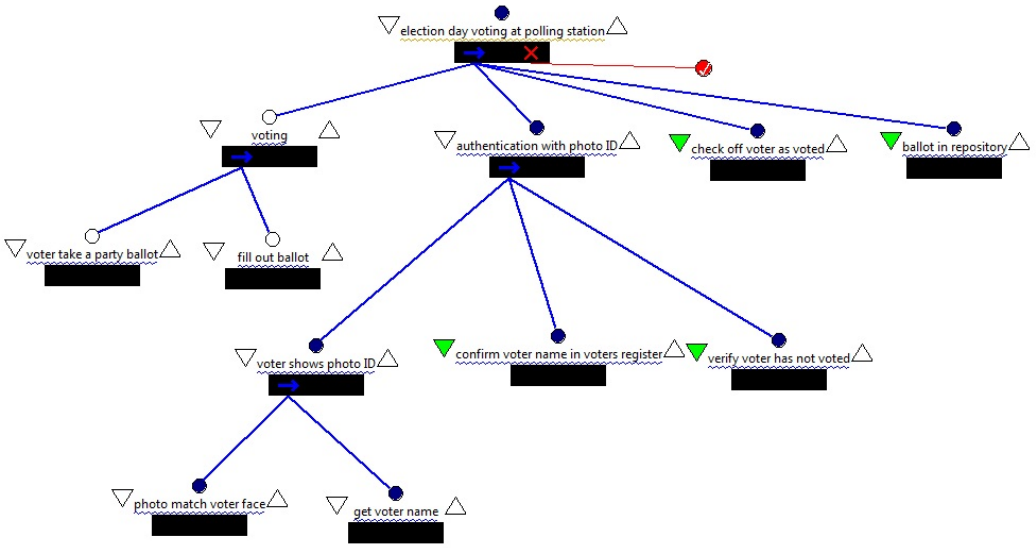

Figura 4.2 – *Modello del processo di voto ai seggi.*

infatti la norma più diffusa è prima controllare l'identità di un elettore e poi, in caso di verifica positiva, fornire una scheda per il voto.

Il secondo figlio dello step principale è *authentication with photo ID*, anch'esso sequenziale, e rappresenta la fase di autenticazione dell'elettore. Questo step ha tre figli, che comunicano tra loro tramite passaggio di parametri (non visibile nel diagramma) e verifica di pre-requisiti.

Nel primo figlio viene chiesto all'elettore il documento con foto e viene preso il suo nome. Lo step *photo match voter face* genera un parametro (*faceOk*) per valutare l'esito positivo del match tra fotografia e volto dell'elettore, e tale parametro viene passato al secondo figlio di *authentication with photo ID*. Nel secondo figlio uno dei triangoli, quello a sinistra, è verde: significa che è presente un pre-requisito da valutare prima che lo step possa iniziare la propria esecuzione. Il pre-requisito in questione è proprio la conferma di match tra fotografia e volto dell'elettore. In caso negativo viene lanciata un'eccezione, in caso positivo invece lo step esegue, comunicando allo step successivo 8tramite parametro *voterRegistered*)se l'elettore è presente nel registro.

Infine, lo step *verify voter has not voted* valuta come pre-requisito che l'elettore sia presente nel registro, e in caso sia presente procede a verificare che non abbia già votato, generando un parametro (*voterQualified*) che verrà passato a *check off voter as voted*.

Lo step *check off voter as voted* valuta come pre-requisito il parametro che gli viene passato e, in caso l'elettore non avesse ancora votato, segna nel registro che ha espresso il suo voto e genera una conferma per lo step successivo, *ballot in repository*, che se positiva da il permesso di mettere la scheda dell'elettore nell'urna.

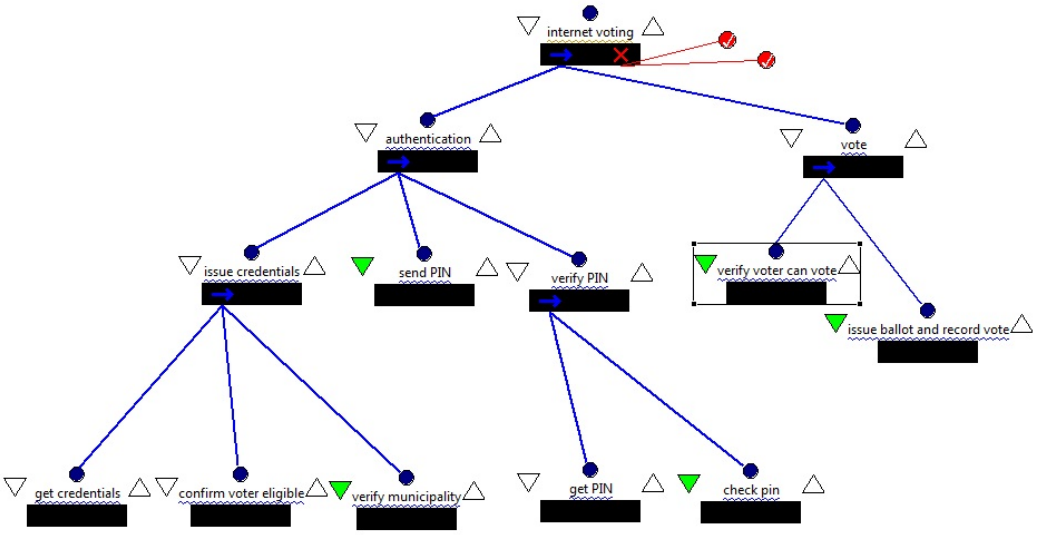

Figura 4.3 – *Modello del processo di voto tramite internet.*

In figura 4.3 è mostrato il diagramma relativo al processo di voto tramite internet. Lo step più in alto, *internet voting*, è uno step sequenziale con due figli, *authentication* e *vote* , ed è un substep dello step *advance voting* visto in figura 4.1.

Authentication è uno step sequenziale che rappresenta l'autenticazione dell'utente nel sistema di voto elettronico norvegese, tramite username e password, utilizzati anche per altri servizi statali, e un PIN. Ha tre figli, *issue credentials*, *send PIN* e *verify PIN*.

Lo step *issue credentials* è uno step sequenziale con tre figli: il primo rappresenta l'inserimento delle credenziali da parte dell'elettore, il secondo la verifica della correttezza delle credenziali inserite, mentre il terzo si occupa di verificare il comune dell'elettore, in quanto solo dieci comuni norvegesi erano stati selezionati per poter utilizzare l'internet voting.

Il secondo figlio, *confirm voter eligible*, genera una conferma che viene valutata come pre-requisito dallo step *verify municipality*, che a sua volta tramite il parametro *voterOk* comunica allo step *send PIN* se l'elettore ha diritto al voto.

Lo step send PIN, nel caso di corretta autenticazione dell'elettore, rappresenta l'invio tramite SMS al suo telefono cellulare di un PIN che l'utente dovrà inserire. Lo step *verify PIN* rappresenta invece l'inserimento del PIN da parte dell'utente e sua verifica da parte del sistema (nello step *check pin*), e un parametro *pinOk* viene mandato fino allo step *verify voter can vote*, che lo controlla come pre-requisito.

Nel caso di esito del controllo positivo, viene creata una conferma di voto per lo step *issue ballot and record vote*.

4.3 Fault Tree Analysis del modello

Uno dei requisiti di un processo di voto è che solo gli elettori qualificati possano votare. Un elettore qualificato è un elettore che ha diritto di voto e che non ha ancora votato. Applicando la Fault Tree Analysis al modello del processo di voto e specificando come pericolo un elettore non qualificato riesce a votare ci si aspetta di far venire alla luce alcune vulnerabilità che un attaccante potrebbe sfruttare.

Il tool per la Fault Tree Analysis, fornito come strumento di analisi per Little-JIL tramite Eclipse, permette di modellare un pericolo di interesse come un parametro che sia un input (o un output) non corretto per un determinato step.

Prendendo in considerazione il diagramma relativo al voto ai seggi il giorno dell'elezione, è possibile modellare il pericolo citato sopra come: *Artifact voterCanVote to ballot in repository is wrong*, dove *voterCanVote* è il parametro che dice se l'elettore può votare, e *ballot in repository* è lo step che riceve quel parametro in input e lo valuta, per permettere eventualmente l'inserimento della scheda nell'urna.

Con il pericolo così definito, il tool produce un fault tree di 33 nodi e 26 gates. Basandosi sul fault tree calcolato, il tool deriva 4 MCSes, di cui tre di grandezza 4 e uno di grandezza 3, indicando quindi che ci sono 4 combinazioni di eventi che possono portare al pericolo, le prime tre sono combinazioni di quattro eventi, e l'ultima è una combinazione di tre eventi. Questo è già un risultato positivo, che indica che nel modello non sono presenti Single Points of Failure.

Da questi MCSes e dal fault tree vengono poi calcolati automaticamente quattro fault tree ognuno relativo a un MCS.

La difficoltà di questa analisi sta nell'interpretazione di ogni MCS, perchè anche se è vero che ogni MCS indica quali eventi del modello possono portare al pericolo, il compito non banale è interpretarli e capire in quale modo possono verificarsi nel processo.

In figura 4.4 è riportato una versione astratta del fault tree, contenente soltanto i nodi di uno dei MCSes di dimensione 4.

L'evento *Exception FaceMismatchException is not thrown by step confirm voter name in voters register* può essere interpretato come una effettiva corrispondenza del volto dell'elettore con quello della fotografia sul documento. Lo step successivo nel diagramma, a cui viene passata la conferma che i volti corrispondono, è *confirm voter name in voters register*. Nel fault tree relativo al MCS viene mostrato che questo step non genera nessuna eccezione: una ipotesi può essere che l'elettore presentatosi abbia un elettore omonimo in quel distretto elettorale, e quindi il suo nome sia presente nel registro. A questo punto viene data la conferma della registrazione dell'elettore e pas-

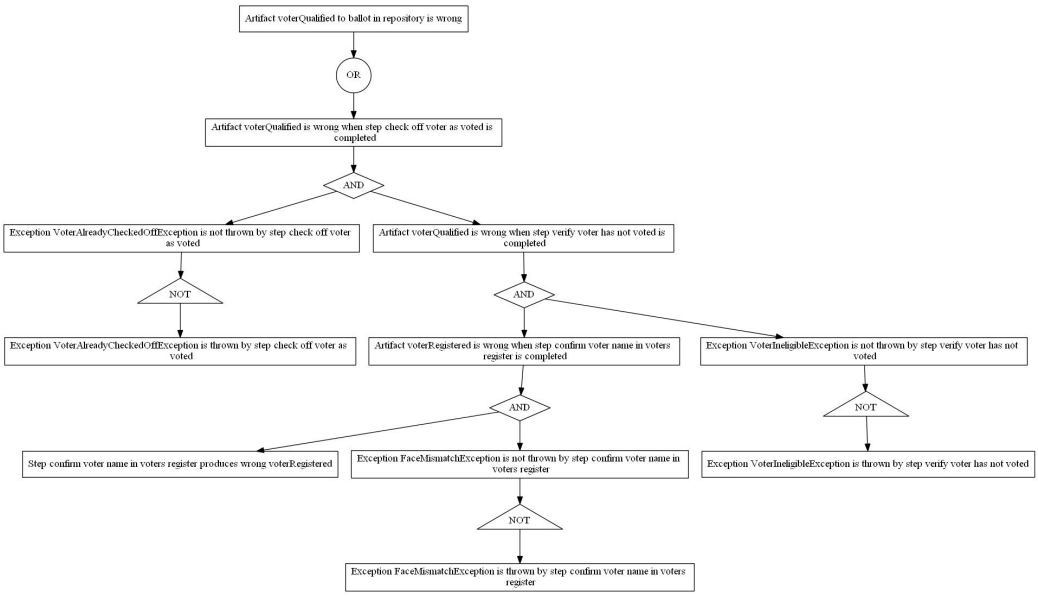

Figura 4.4 – *Fault tree di un MCS di dimensione 4 relativo al voto nel seggio.*

sata allo step successivo, *verify voter has not voted*. Nel fault tree si vede che questo step non genera eccezione, ipotizziamo che sia perchè l'elettore omonimo non abbia ancora votato. A questo punto viene generata la conferma che l'elettore è qualificato per votare (parametro *voterQualified*) e viene passata al successivo step, *check off voter as voted*, che non solleverà nessuna eccezione, e lo step *ballot in repository* si troverà con un parametro di fatto sbagliato.

In questo scenario quindi un impostore sfrutta il fatto di essere omonimo di un elettore correttamente registrato, e non che non ha ancora votato, per riuscire a votare.

Un altro scenario potrebbe essere quello in cui un attaccante non registrato fornisce il proprio documento con nome e fotografia correttamente, e grazie alla complicità degli agenti che si occupano degli step *confirm voter name in voter register* e *verify voter has not voted* (che nel sistema reale potrebbero anche essere compiuti da una singola persona), che ignorano la non presenza del suo nome nel registro, riesce a qualificarsi per votare.

Di seguito vengono presentati i fault tree dei restanti MCSes relativi al voto al seggio.

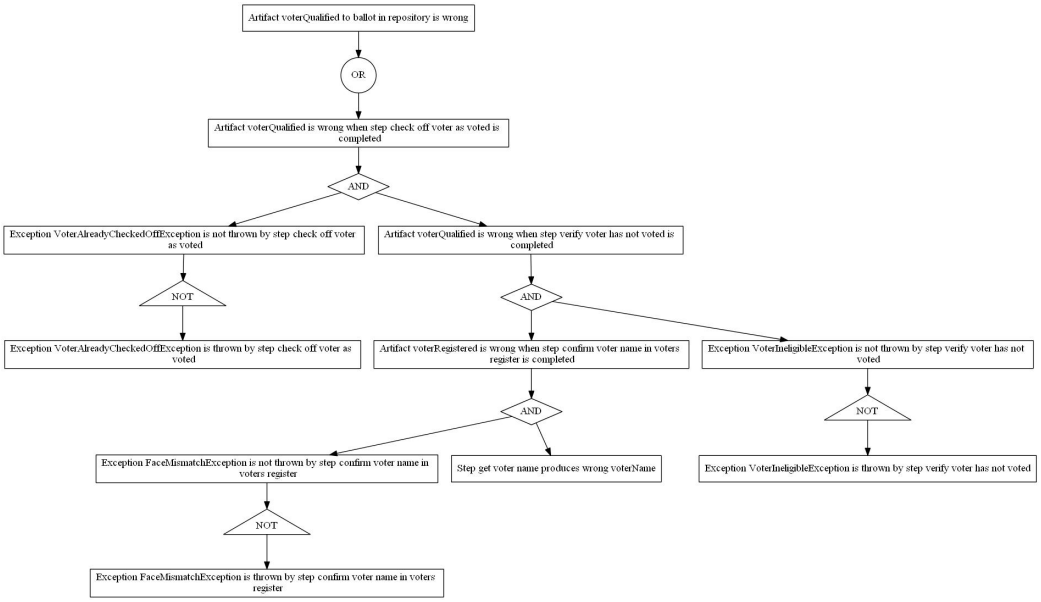

Figura 4.5 – *Fault tree di un MCS relativo al voto nel seggio.*

Nel fault tree di figura 4.5 l'unico scenario in cui potrebbe verificarsi il pericolo è quello in cui il membro dello staff del seggio che si occupa di controllare fotografia e nome sia in realtà complice dell'attaccante. *Exception FaceMismatchException is not thrown by step confirm voter name in voters register* e *Step get voter name produce wrong voterName* significano che il controllo sul volto dell'elettore non ha dato esito negativo, ma il nome è concettualmente sbagliato, probabilmente appartenente a un regolare elettore avente diritto al voto. Siccome sarebbe poco profittevole per l'attaccante recarsi al seggio sperando in un errore dei membri dello staff, l'interpretazione più corretta è che il membro incaricato dei controlli sia suo complice. Le altre considerazioni sul fault tree sono analoghe a quelle fatte in precedenza.

Il MCS di figura 4.6 risulta interpretabile solo nel caso di complicità di un membro dello staff del seggio, che deve essere l'addetto al controllo al registro degli elettori per verificare se l'elettore è presente e se ha già votato,

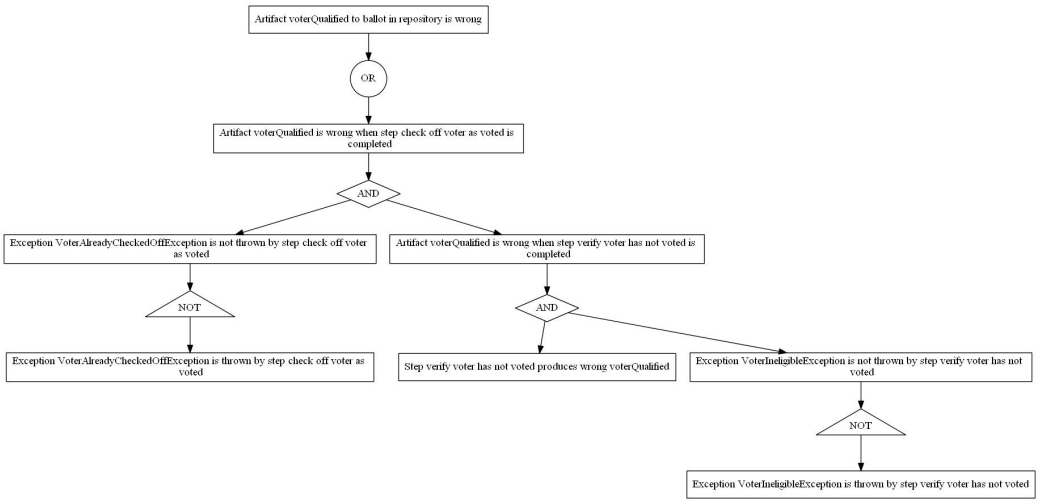

Figura 4.6 – *Fault tree di un MCS relativo al voto nel seggio.*

e deve inoltre essere sempre lo stesso membro a segnalare nel registro che l'elettore ha votato. Si tratta quindi di un MCS di rara utilità pratica, in quanto solitamente diversi membri collaborano in queste funzioni, ed essendo solitamente persone di interessi politici differenti è poco probabile una complicità tra essi.

Anche l'ultimo MCS, in figura 4.7, ha un'interpretazione (simile a quella del MCS relativo alla figura 4.5) basata sulla complicità di uno o più addetti nel seggio. Non viene sollevata nessuna eccezione relativa al riconoscimento del volto, viene fatto passare l'attaccante come presente nel registro, e non viene generata eccezione neanche quando si controlla se l'elettore ha gia votato.

Prendendo in considerazione invece il diagramma relativo all'internet voting, il pericolo di cui si è parlato sopra può essere modellato come *Artifact voterCanVote to issue a ballot and record vote is wrong*, dove *voterCanVote* è il parametro che dice se l'elettore può votare dopo aver verificato la correttezza dell'autenticazione tramite PIN, e *issue a ballot and record vote* è lo step che riceve quel parametro in input e lo valuta, per permettere all'elettore di vedere la scheda elettronica e esprimere il suo voto.

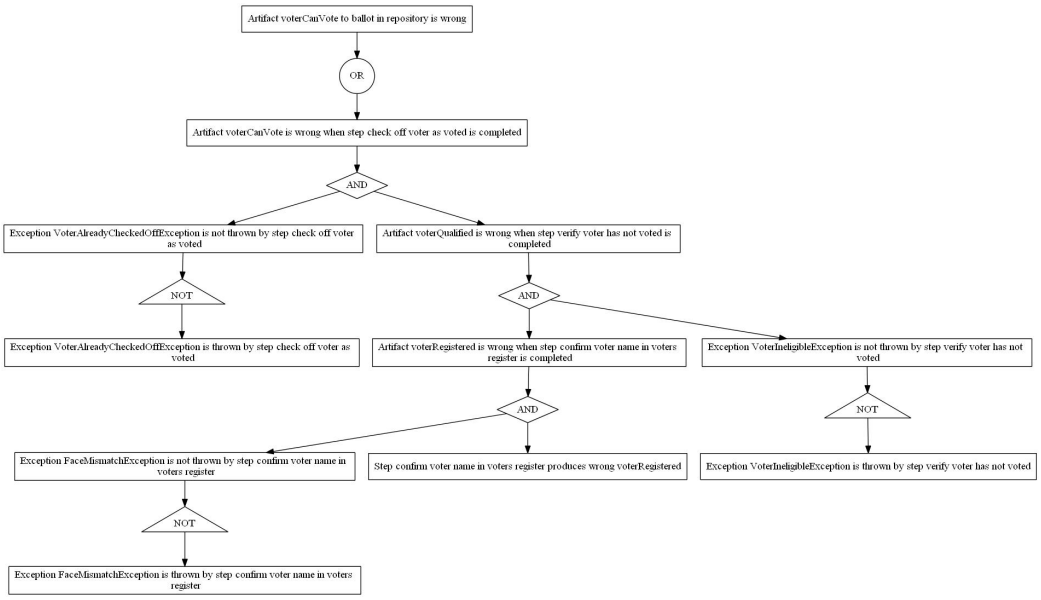

Figura 4.7 – *Fault tree di un MCS relativo al voto nel seggio.*

Il tool per il calcolo del fault tree produce un albero di 54 eventi e 44 gates, e un totale di 6 MCSes, con dimensione da 3 a 5.

In figura 4.8 è riportato il fault tree relativo a uno degli MCS di dimensione 5.

L'evento *Exception WrongCredentialsException is not thrown by step verify municipality* insieme all'evento *Step get credentials produces wrong credentials* può essere interpretato come il fornire da parte dell'attaccante delle credenziali corrette relative a un elettore in una delle municipalità selezionate per l'internet voting, ma che non sono le sue (per questo considerate wrong credentials).

L'elettore visto dal sistema sarà un elettore correttamente registrato, quindi lo step *send PIN* non genera eccezioni e invia il PIN al telefono cellulare dell'elettore. Per lo stesso motivo lo step *check pin* non genera eccezione quando valuta il pre-requisito.

Nell'interpretazione presentata per questo scenario, il fatto che *pinOk* sia non corretto una volta terminato lo step *check pin* significa che l'attaccante

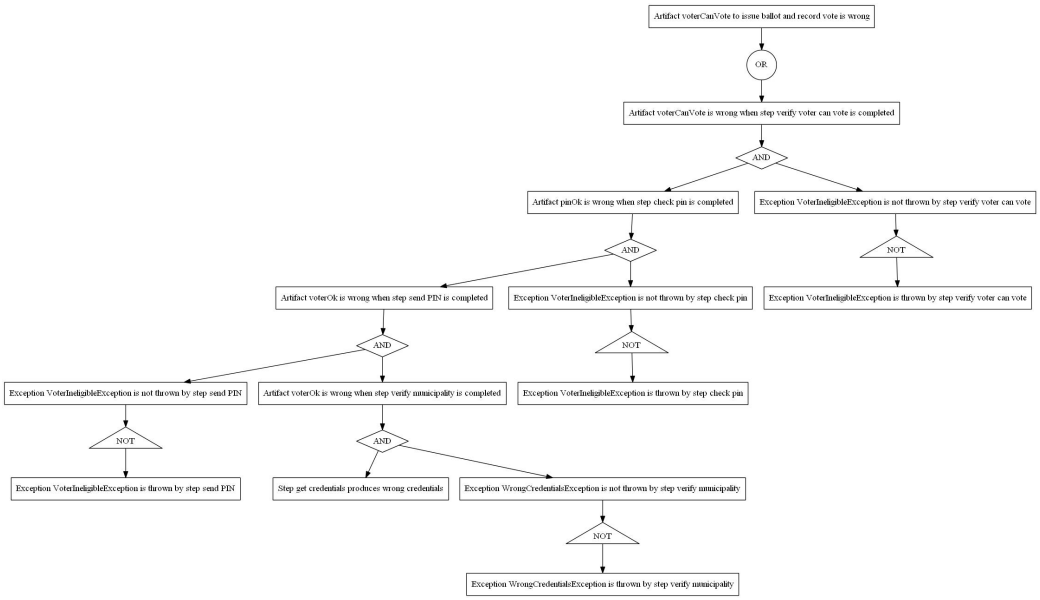

Figura 4.8 – *Fault tree di un MCS di dimensione 5 relativo al voto tramite internet.*

si è in qualche modo impossessato del PIN inviato al telefono dell'elettore correttamente registrato (ad esempio, procurandosi direttamente il telefono, o ottenendo il PIN in qualche altro modo) e l'ha inserito correttamente nel sistema. A questo punto *pinOk* ha valore *true*, ma è concettualmente errato questo valore perchè fa parte di una catena di autenticazione che è stata violata.

Questo valore di *pinOk* fa si che lo step *verify voter can vote* non lanci eccezioni, e la scheda elettronica sarà fornita all'attaccante.

Lo scenario riportato è abbastanza articolato in quanto l'attaccante deve essere in grado di procurarsi credenziali e in qualche modo PIN dell'elettore corretto. Inoltre vale la pena ricordare che nel sistema di internet voting norvegese un elettore può votare tramite internet quante volte desidera, e successivamente saranno scartati tutti i voti elettronici tranne il più recente. Inoltre, votando tramite scheda cartacea, un elettore che ha il dubbio che le sue credenziali siano state rubate è sicuro che i suoi voti elettronici non

verranno conteggiati.

Nelle figure da 4.9 a 4.13 sono rappresentati i fault trees relativi agli altri MCSes relativi al voto tramite internet.

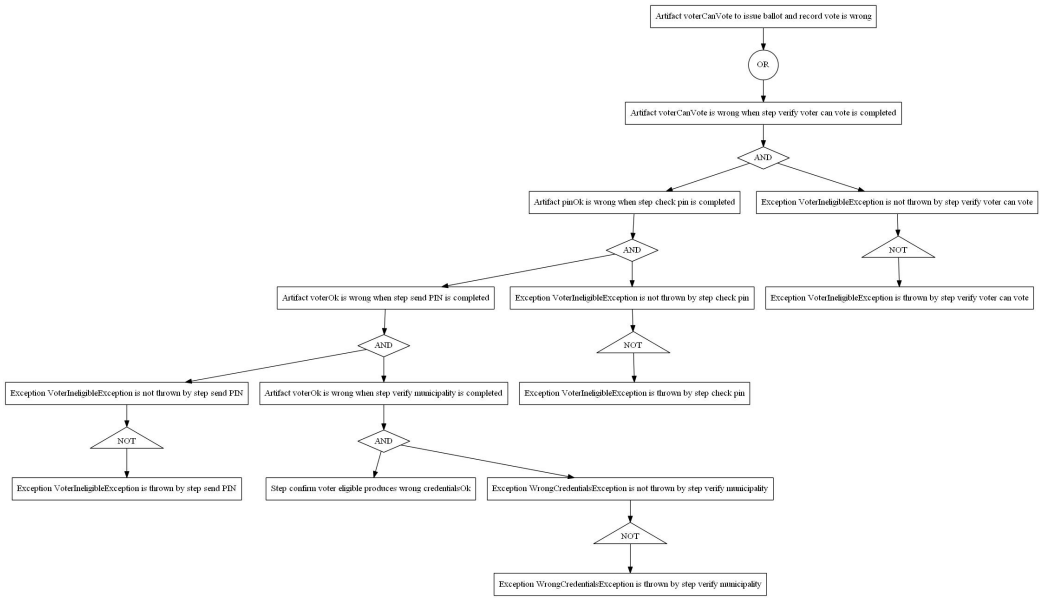

Figura 4.9 – *Fault tree di un MCS di dimensione 5 relativo al voto tramite internet.*

Questi sono difficilmente interpretabili per mancanza di dettagli sull'implementazione del sistema di voto elettronico: ad esempio in figura 4.12 si nota l'evento *step check pin produces wrong pinOk*, ma senza ulteriori dettagli riguardanti il sistema non è possibile sapere cosa possa portare alla generazione di un valore errato. Considerazioni simili valgono per tutti i MCSes restanti, anche se possono comunque essere utili a chi ha una più ampia conoscenza del sistema in questione.

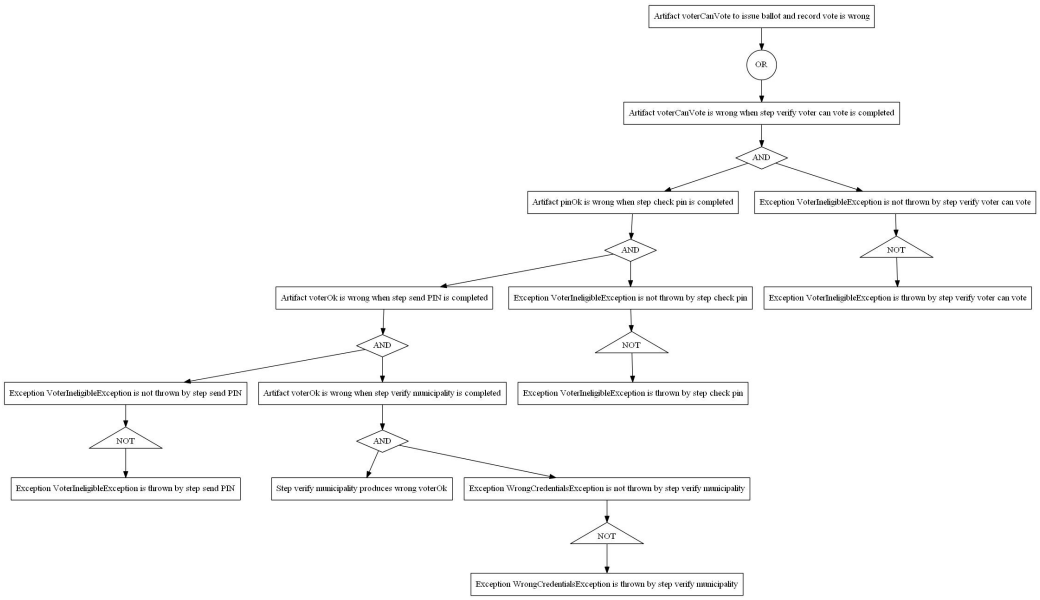

Figura 4.10 – *Fault tree di un MCS di dimensione 5 relativo al voto tramite internet.*

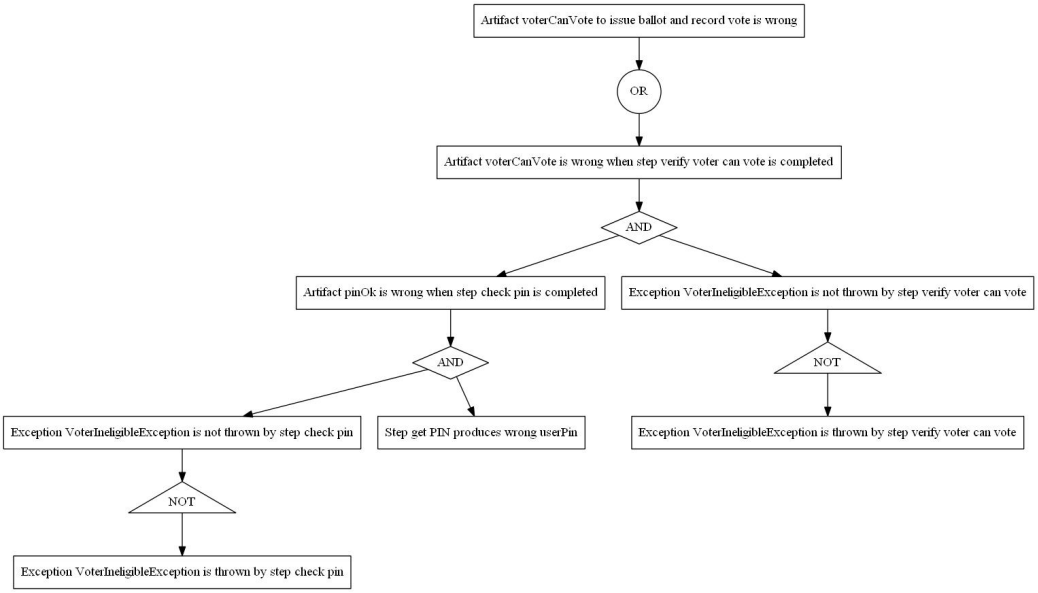

Figura 4.11 – *Fault tree di un MCS di dimensione 3 relativo al voto tramite internet.*

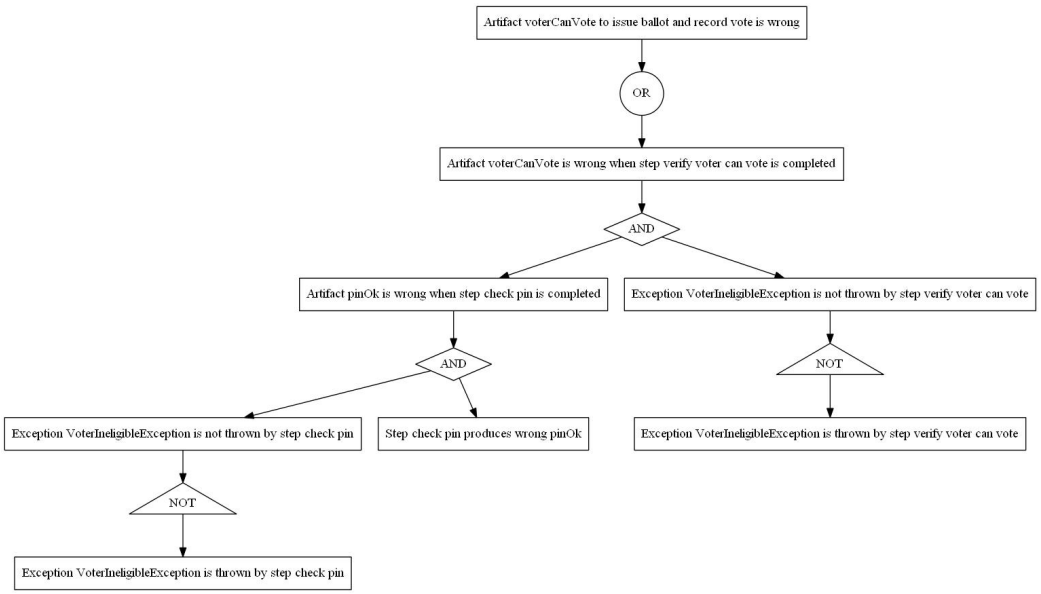

Figura 4.12 – *Fault tree di un MCS di dimensione 3 relativo al voto tramite internet.*

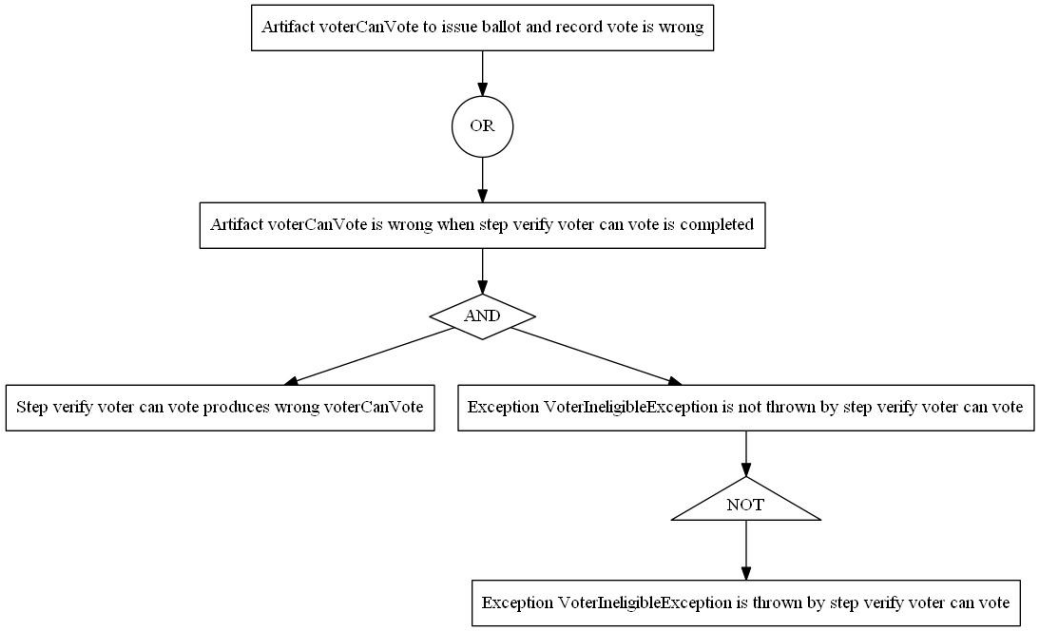

Figura 4.13 – *Fault tree di un MCS di dimensione 2 relativo al voto tramite internet.*

Proposta di miglioramento

La Fault Tree Analysis si rivela uno strumento utile perchè, mostrando possibili vulnerabilità del processo in esame, permette di studiare miglioramenti da introdurre al processo stesso e di verificare la bontà di tali miglioramenti applicando al nuovo processo la FTA.

Dal momento che il sottoprocesso di voto al seggio è quello su cui si hanno maggiori informazioni, in questa sottosezione viene proposto un suo possibile miglioramento per cercare di aumentare le dimensioni dei MCSes, che equivale a renderlo più robusto.

La modifica proposta, considerando anche l'esempio citato in precedenza, è quella di aggiungere, dopo aver verificato la presenza dell'elettore nel registro, la corrispondenza tra l'indirizzo presente nel documento e quello relativo alla residenza dell'elettore registrato. Nella figura 4.14 seguente viene proposto il nuovo modello.

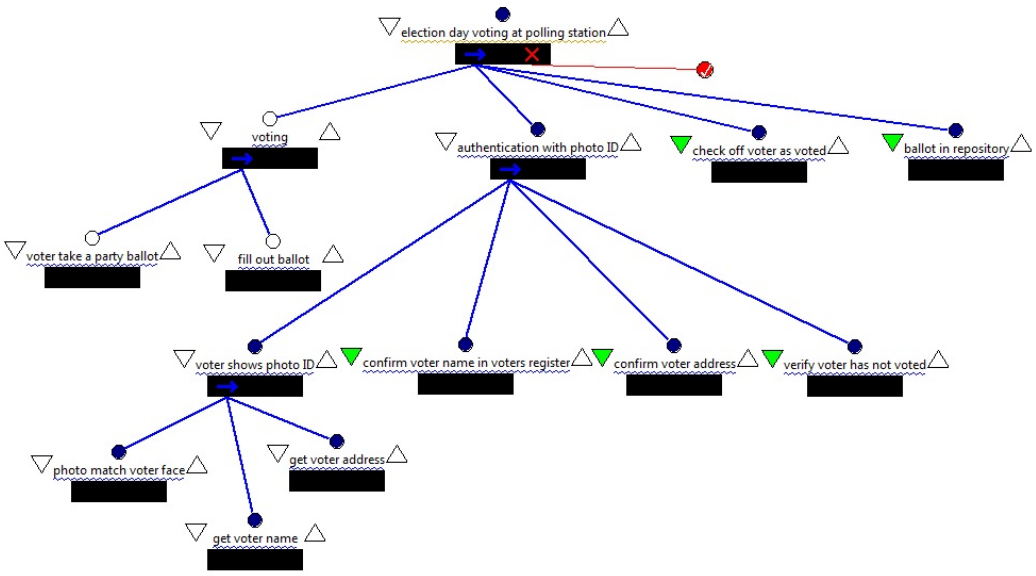

Figura 4.14 – *Modello del processo di voto ai seggi aggiornato con controllo dell'indirizzo.*

Eseguendo la Fault Tree Analysis su questo nuovo modello, ovviamente

specificando come pericolo lo stesso utilizzato in precedenza, e ricalcolando grazie al tool i vari MCSes e i loro relativi fault trees, si nota che il numero dei MCSes è aumentato, da 4 a 6, ma è aumentata anche la loro dimensione: quattro sono di grandezza 5, uno di grandezza 4 e uno di grandezza 3. L'aumento del numero di MCSes potrebbe far pensare a un peggioramento della robustezza, ma la maggior parte di essi ha dimensione 5, ossia devono verificarsi 5 eventi perchè si arrivi al pericolo. Si può dire quindi che in quei casi il verificarsi del pericolo sia davvero molto improbabile.

La nota negativa del miglioramento apportato è che non ha contribuito a migliorare la dimensione del MCS più debole, ossia quello che aveva grandezza minore, in questo caso 3.

Il miglioramento quindi ha portato a un irrobustimento generale del processo tranne che nel caso del MCS di dimensione minore.

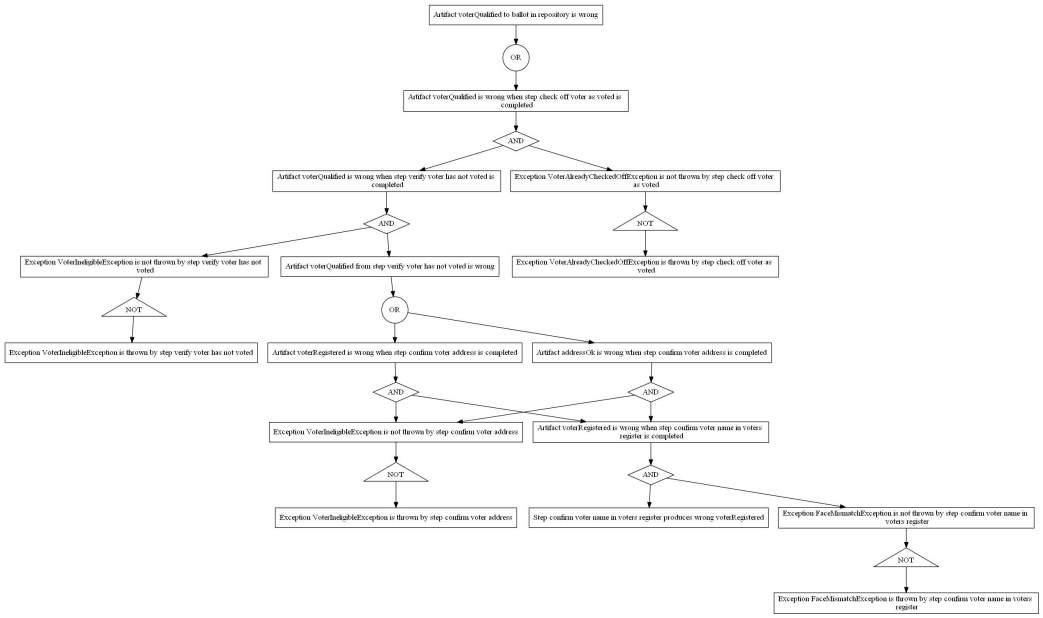

Figura 4.15 – *Fault tree del MCS esaminato precedentemente, aggiornato al nuovo modello.*

Nella figura 4.15 viene proposto il fault tree del MCS esaminato in precedenza in questo capitolo relativamente al voto al seggio, aggiornato al nuovo

modello.

La dimensione in questo specifico MCS è passata da 4 a 5, quindi è leggermente più robusto rispetto alla versione precedente del modello.

4.4 Risultati

L'obiettivo iniziale era cercare di applicare la metodologia utilizzata per modellare il processo di voto a Yolo County, anche a processi di altre parti del mondo, in questo caso quello norvegese.

Si è riusciti con successo a modellare il processo norvegese (nelle parti su cui ci si è concentrati, voto al seggio e internet voting) con gli stessi strumenti, senza particolari difficoltà legate alla metodologia. Questo porta a concludere che sicuramente la metodologia è adeguata almeno per questo processo, non è possibile affermare che lo sia per i processi di ogni parte del mondo, ma cercare di modellarne altri è una buona strada da seguire per verificare la validità generale del metodo.

I fault trees sono stati calcolati partendo dalla stessa minaccia usata per il processo americano, ossia un attaccante non autorizzato a votare riesce a votare. Questa probabilmente è il pericolo più classico che può venire in mente nel contesto di un processo di voto, e il riuscire a specificarla in entrambi i modelli è una maggior conferma della validità del metodo anche su processi diversi.

Analizzando il processo norvegese, definendo il pericolo detto sopra e ricavando i fault trees dei MCSes, si nota che non c'è nessun Single Point of Failure. Questo è un risultato apprezzabile, significa che non esiste un evento singolo che possa portare al verificarsi del pericolo. Le dimensioni dei MCSes per entrambi i casi esaminati (internet voting e voto al seggio) vanno da 3 a 5, un risultato positivo in quanto sta a significare che perchè il pericolo abbia luogo serve almeno una combinazione di tre eventi, e di

conseguenza la probabilità che ciò accada è bassa (si abbassa all'aumentare della dimensione).

Col miglioramento proposto per il voto nel seggio, ossia aggiungere un controllo sull'indirizzo dell'elettore che si presenta al seggio, non viene aumentata la dimensione minima dei MCSes, che rimane 3, ma viene aumentata quella di alcuni MCSes intermedi di dimensione 4, che passano a 5. Questo corrisponde a un irrobustimento del processo riguardo certe combinazioni di eventi, ma non è più sicuro in assoluto in quanto il minimo è comunque 3 come in precedenza.

Conclusioni

In questa tesi è stato presentato un approccio per la modellazione e analisi di processi di voto. Questo approccio era già stato usato con successo per modellare il processo di Yolo County in California. Il metodo consiste nel modellare il processo tramite un linguaggio di modellazione di processi, Little-JIL, e nell'applicare a questo modello un'analisi basata sui fault trees e Minimal Cut Sets.

Come caso di studio, l'approccio descritto è stato applicato al processo di voto utilizzato in Norvegia, con l'obiettivo doppio di verificare se il metodo è abbastanza generale e quindi adatto ad essere applicato a processi di varie parti del mondo, e nel contempo avere una stima della vulnerabilità del processo norvegese, cercando se necessario di migliorarlo.

L'obiettivo è stato in parte raggiunto: data la complessità di un processo elettorale, si è deciso per quello norvegese di concentrarsi su due suoi sottoprocessi, quello di voto al seggio e quello di voto tramite internet. Considerando questi sottoprocessi, il metodo è risultato facilmente applicabile, non sono state incontrate delle difficoltà nella creazione del modello e inoltre il processo norvegese si è dimostrato abbastanza robusto, non avendo neanche un Single Point of Failure ma anzi avendo Minimal Cut Sets di dimensione 3 o superiore. Il miglioramento proposto per cercare di aumentare la dimensione dei MCSes relativi al voto nel seggio ha avuto in parte buon esito: ha irrobustito in generale il processo, portando la dimensione di vari MCSes da 4 a 5, ma non ha migliorato la dimensione del MCSes più debole che rimane

3.

Per completare totalmente la verifica dell'obiettivo, in futuro sarebbe consigliabile di estendere l'approccio all'intero processo, e anche a processi di altri Paesi come quelli descritti nel capitolo 3 (Olanda, Estonia, Svizzera), in modo da avere una maggior autorevolezza dei risultati.

Un'altra strada, indubbiamente interessante, è studiare altri tipi di minacce da modellare e da cui ricavare i fault trees e i MCSes. Oltre a quella più classica vista in questo lavoro, si potrebbe riflettere su quali altri tipi di attacchi o disagi possono creare problemi. Un esempio è cercare di capire se esiste la possibilità che un attaccante possa creare una sorta di Denial of Service contro un sottoinsieme di elettori, magari di cui conosce l'orientamento politico, negandogli la possibilità di votare.

In aggiunta, si potrebbero cercare somiglianze tra i processi (o sottoprocessi) di Yolo County e Norvegia, e anche tra quelli che saranno modellati in futuro, con l'idea di creare dei moduli di processo riutilizzabili in vari processi di voto, con il vantaggio di essere già analizzati e eventualmente resi più sicuri. Tra il processo di Yolo County e i due sottoprocessi di quello norvegese modellati in questa tesi non ci sono somiglianze degne di nota, a causa di differenti metodi di autenticazione e diverso ordine delle procedure di voto, ma l'idea resta comunque valida.

Ci sono anche altri spunti di riflessione interessanti, legati sempre al voto elettronico ma non direttamente collegati a questa tecnica di modellazione. Ad esempio, il voto tramite internet, come in Norvegia, viene effettuato da macchine non controllate, delle quali l'organo elettorale non ha modo di verificare la sicurezza. Se in queste macchine fosse presente un malware creato appositamente, potrebbe cambiare la scelta di voto dell'elettore. Sarebbe interessante ragionare su possibili misure contro questa eventualità. Con in mente il processo norvegese, si potrebbe ad esempio pensare di inviare in modo automatico al telefono cellulare dell'elettore un SMS con indicato il voto espresso. Si potrebbe discutere sul fatto che la segretezza del voto

potrebbe venire meno, è un server che deve decifrare il voto dell'elettore, ma vedendo nel messaggio ricevuto un voto diverso da quello espresso l'elettore avrebbe la possibilità di votare da un'altra macchina o di recarsi al seggio se possibile (da ricordare che nel processo di voto norvegese è possibile votare tramite internet quante volte si vuole, e se si vota anche al seggio il voto cartaceo annulla quelli elettronici).

Un'altra tipologia di voto tramite internet, non trattata in questa tesi, è il voto tramite mail. Anche questa tipologia richiede riflessioni accurate, in quanto uno dei problemi che si possono verificare, e in alcuni casi è stato così, è il riempimento della casella. Questo ovviamente porterebbe al rifiuto dei voti degli elettori che li inviano successivamente al rimepimento. Una soluzione potrebbe essere un adeguato sistema di inoltro ad un appropriato numero di caselle di supporto, soluzione che comunque richiederebbe studi sul numero mail che si potrebbero ricevere.

Bibliografia

[1] R.M. Alvarez, T.E. Hall, and A.H. Trechsel. Internet voting in comparative perspective: the case of estonia. *PS: Political Science and Politics*, 42(3):497–505, 2009.

[2] A. Ansper, S. Heiberg, H. Lipmaa, T. Øverland, and F. Van Laenen. Security and trust for the norwegian e-voting pilot project e-valg 2011. *Identity and Privacy in the Internet Age*, pages 207–222, 2009.

[3] N. Braun and D. Brändli. Swiss e-voting pilot projects: Evaluation, situation analysis and how to proceed. *Electronic Voting*, pages 51–60, 2006.

[4] A.G. Cass, AS Lerner, E.K. McCall, L.J. Osterweil, S.M. Sutton Jr, and A. Wise. Little-jil/juliette: a process definition language and interpreter. In *Software Engineering, 2000. Proceedings of the 2000 International Conference on*, pages 754–757. IEEE, 2000.

[5] B. Chen, G. Avrunin, L. Clarke, and L. Osterweil. Automatic fault tree derivation from little-jil process definitions. *Software Process Change*, pages 150–158, 2006.

[6] A. Ericson and C. Ll. Fault tree analysis. In *System Safety Conference, Orlando, Florida*, 1999.

[7] OSCE Organization for Security and Co operation in Europe. Elections in estonia. `http://www.osce.org/odir/elections/estonia/`.

[8] OSCE Organization for Security and Co operation in Europe. Elections in netherlands. `http://www.osce.org/odir/elections/netherlands/`.

[9] OSCE Organization for Security and Co operation in Europe. Elections in norway. `http://www.osce.org/odir/elections/norway/`.

[10] OSCE Organization for Security and Co operation in Europe. Elections in switzerland. `http://www.osce.org/odir/elections/switzerland/`.

[11] J. Gerlach and U. Gasser. Three case studies from switzerland: E-voting. *Berkman Center Research Publication No*, 3, 2009.

[12] E. Hubbers, B. Jacobs, and W. Pieters. Ries-internet voting in action. In *Computer Software and Applications Conference, 2005. COMPSAC 2005. 29th Annual International*, volume 1, pages 417–424. IEEE, 2005.

[13] B. Jacobs and W. Pieters. Electronic voting in the netherlands: from early adoption to early abolishment. *Foundations of Security Analysis and Design V*, pages 121–144, 2009.

[14] D.W. Jones. The evaluation of voting technology. *Secure Electronic Voting*, pages 3–16, 2003.

[15] Ü. Madise and T. Martens. E-voting in estonia 2005. the first practice of country-wide binding internet voting in the world. *Electronic voting*, 86, 2006.

[16] H. Phan, G. Avrunin, M. Bishop, L.A. Clarke, and L.J. Osterweil. A systematic process-model-based approach for synthesizing attacks and evaluating them. In *Proceedings of the 2012 international conference on Electronic Voting Technology/Workshop on Trustworthy Elections*, pages 10–10. USENIX Association, 2012.

[17] M. Raunak, B. Chen, A. Elssamadisy, L. Clarke, and L. Osterweil. Definition and analysis of election processes. *Software Process Change*, pages 178–185, 2006.

[18] B.I. Simidchieva, S.J. Engle, M. Clifford, A.C. Jones, B. Allen, S. Peisert, M. Bishop, L.A. Clarke, and L.J. Osterweil. Modeling and analyzing faults to improve election process robustness. In *2010 Electronic Voting Technology Workshop/Workshop on Trustworthy Elections, Washington, DC*, 2010.

[19] B.I. Simidchieva, M.S. Marzilli, L.A. Clarke, and L.J. Osterweil. Specifying and verifying requirements for election processes. In *Proceedings of the 2008 international conference on Digital government research*, pages 63–72. Digital Government Society of North America, 2008.

[20] W.E. Vesely. *Fault tree handbook*. Nuclear Regulatory Commission, 1987.

[21] A. Wise. Little-jil 1.5 language report. department of computer science, university of massachusetts. Technical report, Amherst UM-CS-2006-51, 2006.

[22] Laser Process working Group et al. Getting started with little?jil, 2002.