Utveckling av metod inklusive verktygsstöd för värdering av säkerhetsnivån i driftstödssystem

Slutrapport från ett post-doc-projekt

Elforsk rapport 09:32

Erik Johansson, Pontus Johnson, Mathias Ekstedt, Robert Lagerström, Teodor Sommestad, Johan Ullberg, Ulrik Franke

Februari 2009

ELFORSK

Utveckling av metod inklusive verktygsstöd för värdering av säkerhetsnivån i driftstödssystem

Slutrapport från ett post-doc-projekt

Elforsk rapport 09:32

Erik Johansson, Pontus Johnson, Mathias Ekstedt, Robert Lagerström, Teodor Sommestad, Johan Ullberg, Ulrik Franke

Februari 2009

Förord

Denna rapport är framtagen av projektet ”Utveckling av metod inklusive verktygsstöd för värdering av säkerhetsnivån i driftstödssystem”, inom FoU-programmet Riskanalys 06-10 som drivs av Elforsk AB. Projektet har genomförts som ett post-docprojekt av Erik Johansson, Pontus Johnson, Mathias Ekstedt, Robert Lagerström, Teodor Sommestad, Johan Ullberg och Ulrik Franke, KTH.

Syftet med projektet är att vidareutveckla en metod och utveckla ett verktyg som används till att utvärdera säkerheten i driftstödssystem gentemot IT-säkerhetsstandarden NERC CIP.

Programmets styrgrupp består av följande ledamöter:
Arne Bergström, Vattenfall Eldistribution AB
Horst Blüchert, Elsäkerhetsverket
Mikael Bohjort, E.ON Elnät Sverige AB
Leif Boström, Fortum Distribution
Håkan Jarer, Svenska Kraftnät
Sven-Åke Polfjärd, Föreningen Industriell Elteknik, FIE
Sven Jansson, Elforsk AB, programansvarig

Finansiärer i programmet är:
Vattenfall Eldistribution AB
E.ON Elnät Sverige AB
Fortum Distribution AB
Svenska Kraftnät
Göteborg Energi AB
Skellefteå Kraft AB
Mälarenergi Elnät AB
Tekniska Verken i Linköping AB
Öresundskraft AB
Jämtkraft AB
Umeå Energi AB
Jönköpings Energi Nät AB
Eskilstuna Energi & Miljö AB
Gävle Energi AB
Energiverken i Halmstad AB
Sundsvall Elnät AB
Växjö Energi Elnät AB
Borlänge Energi AB
Nacka Energi AB
Föreningen Industriell Elteknik, FIE
Elsäkerhetsverket
Lunds Energi AB

Projektets referensgrupp består av följande ledamöter:
Per Clasén, E.On
Georg Karlén, Vattenfall
Dr. Göran Ericsson, Svenska Kraftnät
Dr. Åke Holmgren, Krisberedskapsmyndigheten
Prof. Torsten Cegrell, Kungliga Tekniska högskolan

Bertil Wahlund
Överföring & Distribution
Elforsk AB

Sammanfattning

Driftstödssystem används för att säkerställa en effektiv och säker eldistribution. Störningar i dessa digitala kontrollsystem är kritiska då de påverkar driften av kraftnätet. Med ökade krav på leveranskvalitet kan kostnaderna för dessa störningar således även komma bli omfattande för distributionsbolagen.

Trots detta saknar idag bolagen verktygsstöd för att identifiera, analysera och prioritera sårbarheter i driftstödsystemen. Sårbarheterna i dagens driftsstödsystem exponeras mot nya typer av hot genom att de i allt högre utsträckning görs tillgängliga via publika nätverk som Internet, dessutom bygger de alltmer på samma teknik som vanliga IT-system och därtill integreras de ofta med administrativa IT-system. Vidare är många av de styrsystem som idag är i drift utvecklade under en tid då IT-säkerhet inte nämnvärt beaktades. Sammanfattningsvis medför den här utvecklingen en radikalt förändrad hotbild som kraftbolag behöver uppmärksamma för att vidta relevanta åtgärder.

Det här post-doc-projektet har dels vidareutvecklat en metod (som forskats fram vid KTH i nära samarbete med Vattenfall) samt dels utvecklat ett verktyg som ger Elforsks intressenter ett stöd i arbetet med att utvärdera säkerheten i driftstödssystem gentemot IT-säkerhetsstandarden NERC CIP.

Summary

Process control systems, also referred to as SCADA (Supervisory, Control and Data Acquisition) systems, are used to ensure an effective and safe distribution of electricity. Disruptions in these SCADA-systems are critical since they affect the power grid operation. With the increased demand for supply, the costs of these disruptions might also become extensive for utilities.

Despite this, companies lack suitable tools to identify, analyze and prioritize vulnerabilities in operational support system. The vulnerabilities of today's SCADA-systems are exposed to new types of threats when they are being made available over public networks such as the Internet. Moreover, they are increasingly based on the same technology as ordinary IT-systems and more often becomes integrated with the administrative IT-systems. In addition, many of the control systems that are in operation today were developed at a time when cyber security was not considered. In conclusion, this development brings a radically different threat that power utilities need to pay attention to in order to take relevant measures.

This post-doc project has on one hand, developed a method (based upon research presented at the Royal Institute of Technology in close collaboration with Vattenfall), and secondly, developed a tool that provides the stakeholders of Elforsk support in the process of evaluating the security of operational support systems towards the cyber security standard NERC CIP.

Innehåll

1 Bakgrund

Transmission och distribution av elkraft är beroende av datorbaserade system för styrning, reglering och övervakning. Dessa datorbaserade system brukar benämnas SCADA-system (Supervisory Control And Data Acquisition). Säkerheten i elkraftsystemet är i allt större omfattning avhängig säkerheten och pålitligheten i SCADA-systemen. Sedan den 11 september 2001 har dessutom oron ökat för intrång i dessa datorbaserade system. Ett sådant intrång skulle i värsta fall kunna leda till att en attackerare övertar kontrollen över elkraftsystemet.

Bakgrunden till detta nya hot är att de industriella styrsystem blir allt mer ihopkopplade med såväl övrig IT-infrastruktur inom företagen som mot Internet. Detta gör att möjligheterna att angripa styrsystem ökat drastiskt under det senaste decenniet. Styrsystemen som används idag är i sig inte heller byggda för att motstå angrepp utan utgår ifrån att användningen av systemen är av godartad karaktär.

Som ett led i arbetet att vidmakthålla och/eller förbättra SCADA-säkerheten är metoder och verktyg för att utvärdera säkerhetsnivån i ett givet system viktiga. Idag saknar industriella beslutsfattare ett bra stöd för att fatta rationella styrsystemssäkerhetsbaserade beslut vilka tar hänsyn till situationen som helhet.

På avdelningen för Industriella informations- och styrsystem på KTH har forskning på SCADA-system för kraftsystemsstyrning bedrivits sedan sent åttiotal. På senare år har avdelningen riktat in sig allt mer mot utvärdering av säkerheten i SCADA-system.

I ett tidigare forskningsprojekt vid avdelningen har en metod, kallad EISAM (Enterprise Information Security Assessment Method), tagits fram för värdering av säkerhetsnivån i informationssystem. Metoden bygger på krav från ett flertal standarder och använder sig av datainsamling och etablerade metoder för beslutsfattande under osäkerhet för att aggregera en total nivå på informationssäkerhet, vilken tar hänsyn till såväl organisatoriska som tekniska aspekter. EISAM-metoden har bland annat presenterats i en doktorsavhandling vid KTH framlagd av Erik Johansson samt vid ett flertal internationella konferenser.

År 2006 erhöll avdelningen finansiering från Elforsk för att utveckla en helt ny typ av verktygsstöd för säkerhetsutvärdering av informationssystem. Detta verktygsstöd baseras på tidigare forskningsresultat vid avdelningen och en vidareutveckling av EISAM-metoden påbörjades.

Denna rapport presenterar resultat från detta post-doc-projekt samt presenterar statusen för verktyget i dess allra första version sommaren 2008.

2 Mål

Det ursprungliga målet med detta forskningsnära post-doc-projekt har varit att vidareutveckla den sk EISAM-metoden så att den blir tillämpbar och tillgänglig genom att ta fram ett datoriserat verktyg. Ett verktyg som kan stödja arbetet att mäta och därmed utvärdera informationssäkerheten i driftsstödsystem.

Under projektets gång har ambitionen ökats till att verktyget inte bara skall kunna stödja EISAM-metoden eftersom den i sig baserar sig på informationssäkerhetsstandarder som med tiden kommer att bli utdaterade. Istället har målet omformulerats till att utveckla ett verktyg som är så pass flexibelt att det kan överleva den hastiga teoretiska utveckling som sker inom informationssäkerhetsområdet. Som referens för säkerhetsstandard har projektet använt North American Electric Reliability Corporation's Critical Infrastructure Protection (NERC-CIP) [4].

De konkreta målen med post-doc-projektet har varit att ta fram tre leverabler, nämligen ett informationssäkerhetsanalysverktyg, en instruktionsbok för verktyget, och ett utbildningspaket.

3 Genomförande

Arbetet med att utveckla verktyget har involverat ett flertal personer på avdelningen på industriella informations- och styrsystem på KTH. Organisationen och arbetsprocesser har utvecklats under projektets gång och omfattar idag en mycket större organisation en den som ursprungligen finansierats av Elforsk. Detta kapitel redovisar den organisation som nu är aktiv i projektet.

3.1 Övergripande organisation och roller

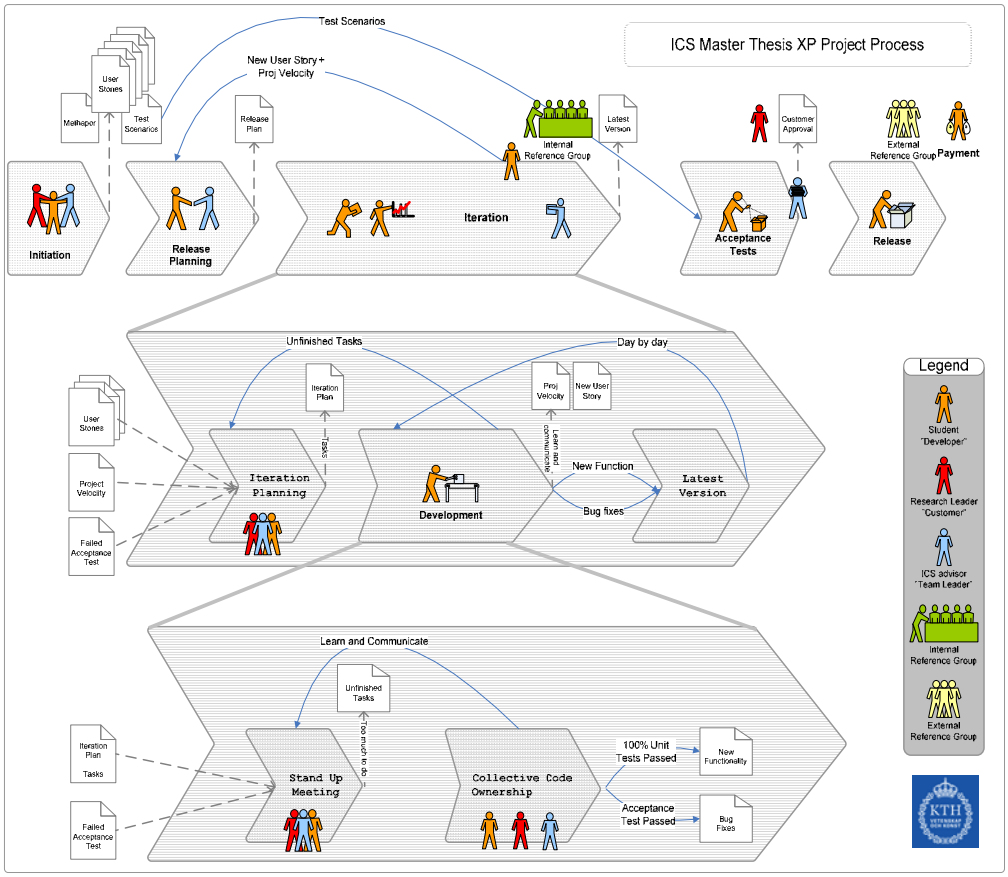
På en övergripande nivå har projektet bestått av fyra intressentgrupper:

- Finansiär. Projektet har finansierats av Elforsk via programstyrelsen i Riskanalys 06 - 10
- Projektgrupp. Projektet har utförts av doktorander och seniora forskare vid industriella informations- och styrsystem. Projektgruppen beskrivs mer utförligt nedan.
- Extern referensgrupp. För att upprätthålla en god industriell relevans i projektet har en extern referensgrupp använts. Viktig input från den externa referensgruppen har varit att anpassa arbetet till den Amerikanska säkerhetsstandarden för styrsystemshantering, NERC-CIP. Fem stycken möten mellan projektgruppen och denna grupp har hållits under projektets löptid. Medlemmar i denna grupp är:
    - Per Clasén, E.On
    - Georg Karlén, Vattenfall
    - Dr. Göran Ericsson, Svenska Kraftnät
    - Dr. Åke Holmgren, Krisberedskapsmyndigheten
    - Prof. Torsten Cegrell, Kungliga Tekniska högskolan
- Intern referensgrupp. För att upprätthålla en god synkronisering med den forskning som bedrivs vid avdelningen har också en intern referensgrupp använts med ett flertal av avdelningens verksamma forskare. Under mötena med den interna referensgruppen har krav på verktyget identifierats och prioriterats.

3.2 Aktiviteter

Projektgruppen, som utfört arbetet med utvecklingen, har bestått av en blandning av examensarbetare, doktorander och seniora forskare. Totalt har hela 14 personer varit involverade i arbetet varav 7 är anställda forskare. Generellt kan arbetet beskrivas i följande sex aktivitetskategorier:

1. Projektledning och extern kommunikation. Denna kategori uppgifter handlar om att synkronisera de olika projektintressenterna med utvecklingsarbetet inom projektgruppen, traditionell projektplanering och uppföljning samt utarbetande av kommunikationsmaterial. Denna uppgift har till största del utförts av Erik Johansson.
2. Kravhantering och övergripande design. Dessa aktiviteter består i att förfina och prioritera de krav på verktyget som kommit från referensgrupperna och utifrån detta skapa ett arkitektoniskt skelett för verktyget. Dessa uppgifter har till största del utförts av Pontus Johnson, Mathias Ekstedt och Robert Lagerström.
3. Förvaltning och utveckling av utvecklingsmiljö. Dessa aktiviteter handlar om att välja installera och uppdatera den miljö och stödprogram som använts i utvecklingen. Miljön har uppdaterats vid ett flertal tillfällen. Dessa uppgifter har till största del utförts av Johan Ullberg och Teodor Sommestad.
4. Utveckling. Denna aktivitet handlar om att producera källkod med tillhörande dokumentation. Dessa uppgifter har till största del utförts av examensarbetare knutna till projektet men samtliga projektmedlemmar har varit involverade i detta.
5. Testning. Denna aktivitet handlar om att kontrollera att den utvecklade koden stämmer med de ursprungliga kraven. Denna uppgift utförts av samtliga projektmedlemmar.
6. Intern handledning. I och med att mycket av utvecklingsarbetet genomförts av examensarbetare har det krävts en hel del handledning av och synkronisering mellan examensarbetarna. Figur 1 nedan illustrerar arbetsflödet för examensarbeten. Denna uppgift har till största del utförts av Ulrik Franke, Johan Ullberg, Teodor Sommestad samt Erik Johansson.



Figur 1. Illustration över arbetsflödet för examensarbeten i projektet.

4 Resultat

Resultaten från projektet redovisas och finns att ladda ner på projektets hemsida:www.ics.kth.se/EAT

Nedan sammanfattas resultaten.

4.1 Datoriserat informationssäkerhetsanalysverktyg

Verktyget, som kan köras på en standard PC med stöd för Java™, underlättar och förbättrar arbetet med att analysera säkerheten i styrsystem. En viktig skillnad mot traditionellt säkerhetsarbete är att verktyget baserar sig på grafiska modeller av systemen, s.k. arkitekturmodeller, och inte på textuella beskrivningar som är det vanliga i t.ex. standarder. Detta gör det väsentligt mycket lättare att få en helhetsförståelse av hur systemen är konfigurerade och sammankopplade med varandra. Detta leder i sin tur att det är enklare att skapa beslutsunderlag som tar helheten i beaktande vilket är nödvändigt för att fatta rationella beslut om säkerhet i styrsystem. En annan viktig egenskap hos verktyget är att det hanterar de osäkerheter som finns i samband med säkerhetsanalyserna. I de komplexa systemmiljöer som finns implementerade i industrin idag är det praktiskt omöjligt att samla in komplett mängd med fullt tillförlitlig information om hur systemen är konfigurerade och hur de hanteras som krävs för att göra en komplett analys av situationen. Den typ av idealistiska modeller och ramverk som förs fram i standarder och akademiska arbeten faller ofta på sin orimlighet. Verktyget kompletterar dessa arbeten med en mekanism (en vidareutveckling av Bayesiansk statistik [3] [6]) för att hantera inkompletthet och osäkerheter i det data som man använder för analysen.

4.1.1 Användning

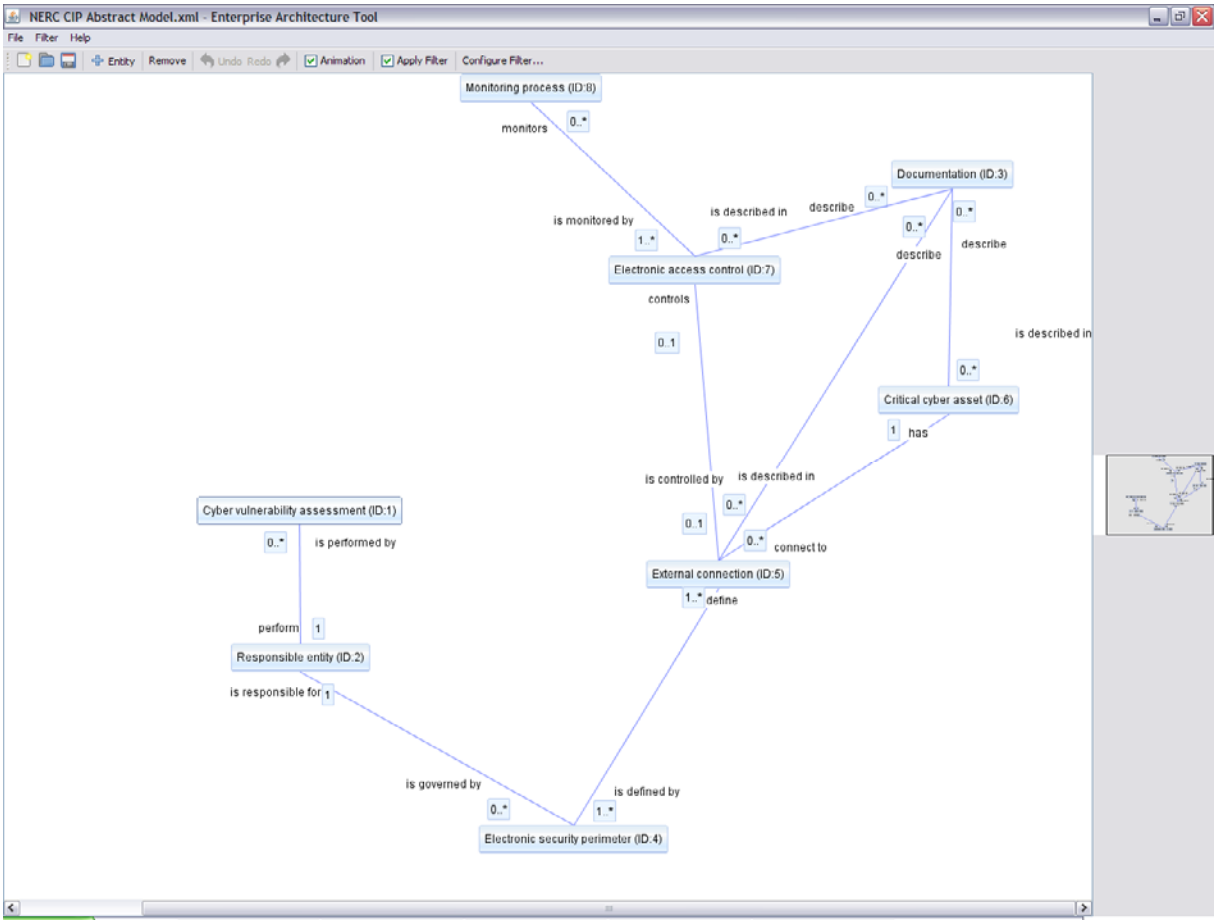
Verktyget består av två delar: den ***abstrakta modelleraren*** och den ***konkreta modelleraren***. I den abstrakta modelleraren specificeras det ramverk, eller den teori, som skall användas som bas för den förestående analysen. I den konkreta modelleraren specificeras sedan, utifrån den generella abstrakta modellen, en specifik modell för ett visst företag och systemscenario. För att göra detta behöver man samla in information om hur systemen och organisationen faktiskt är konfigurerade, alternativt hur man tänkt sig designa framtida scenarion. Vi skiljer alltså på generella klasser av saker och företeelser, som exempelvis ”universitet” – som vi beskriver i den abstrakta modelleraren, och konkreta faktiska instanser av dessa klasser, exempelvis ”KTH” – som vi beskriver i den konkreta modelleraren.

Nedan beskrivs användningen av dessa två delar med hjälp av ett enklare exempel i syfte att ge en förståelse för hur verktyget fungerar i sin helhet.

Den abstrakta modelleraren

Den abstrakta modelleraren är den del av verktyget som används för att specificera abstrakta modeller. Dessa abstrakta modeller dikterar vad som ska modelleras i den konkreta modelleraren, och hur olika värden i den konkreta modellen för utvärderingen ska beräknas. I projektet har som sagt NERC CIP använts som underliggande teoretiskt ramverk. I exemplet här baserar vi oss på en del av ”NERC CIP 005” – den femte delen av standarden.

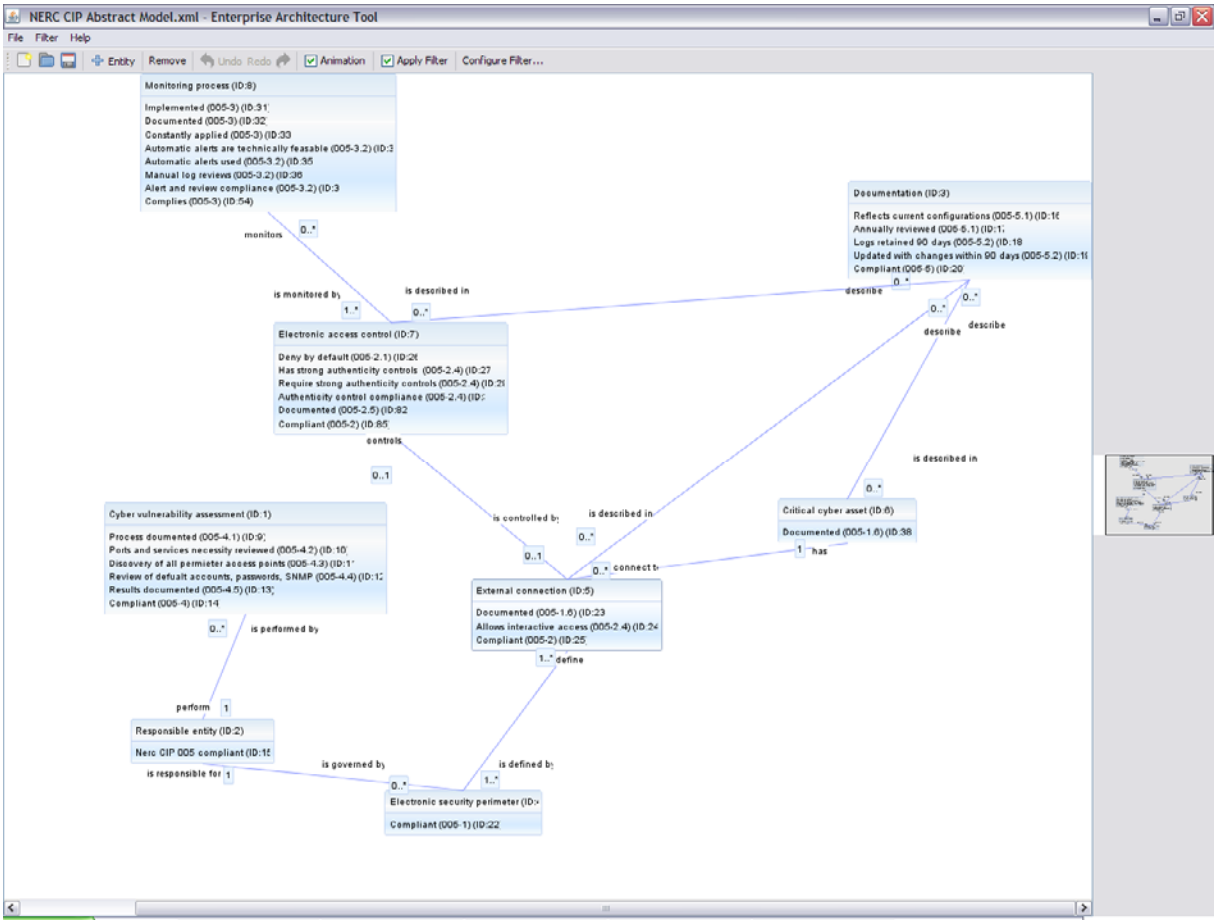
Basen i abstrakta modeller är **entiteter** och **relationer**. Entiteter symboliserar saker och fenomen och relationer specificerar hur dessa entiteter hänger samman. NERC CIP 005 behandlar bland annat hur man skyddar de elektroniska gränserna till det betraktade systemet. I Figur 2 nedan visar en modell över fenomen, av projektet tolkade i entiteter och relationer, som denna del av standarden pratar om. Man kan här t.ex. se att en ”Responsible entity” (se nedre vänstra hörnet) kan utföra ”Cyber vulnerability assessments” och att den ansvariga enheten också ansvarar för ”Electronic security perimeter”. (I varje ände på relationen anges den roll som de olika entiteterna har i förhållande till varandra; tex en ”Responsible entity” ”perform” ”Cyber vulnerability assessments” och vice versa är ”Cyber vulnerability assessments” ”performed by” ”Responsible entity”. Vidare anges en så kallad multiplicitet som anger hur många konkreta instanser av entiteterna som får kopplas till varandra. En utvärdering görs av exakt en ansvarig enhet men den ansvariga enheten kan utföra noll eller flera utvärderingar.) Vidare säger denna abstrakta modell att en ”Electronic security perimeter” definieras av åtminstone en men potentiellt flera (multiplicitet 1..*) ”External connection”. I övre högre delen av figuren kan man se att en sådan ”External connection” är kopplad till en ”Critical cyber asset” (typiskt de IT-system och komponenter som skall skyddas), som kan vara beskriven i ”Documentation” och kan kontrolleras av en ”Electronic access control”. Såväl den elektroniska behörighetskontrollen som en ”Crictical Cyber asset” kan, precis som en ”External connection” vara beskriven i dokumentation, och utöver det kan behörighetskontrollen även vara övervakad av en ”Monitoring process”.



Figur 2. En abstrakt modell av elektroniskt gränssnittsskydd i enlighet med NERC CIP 005 .

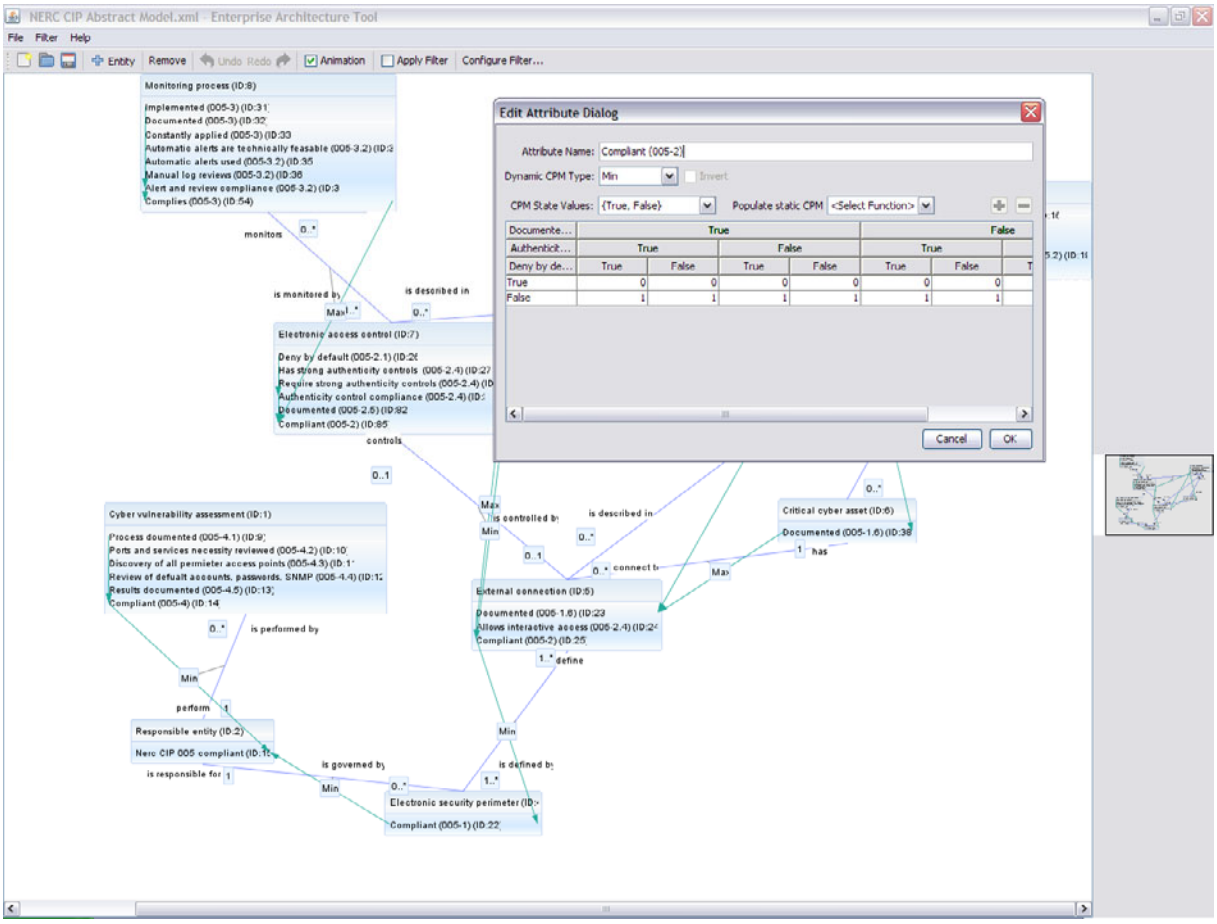
De nyss beskrivna entiteterna och relationerna utgör basen för den abstrakta modellen men utöver dessa bestäms också vilka egenskaper i dessa entiteter som är viktiga för analysen. Dessa kallas i modellen för **attribut.** Figur 3 visar samma modell som i Figur 2 men nu utökad med de attribut som hör till respektive entitet. Här kan man t.ex. se att ett dokument (övre högra hörnet) kan vara årligen granskat eller inte, eller att det den ansvariga enheten (”responible entity”) kan ha egenskapen att vara ”NERC CIP 005 compliant”, dvs om NERC CIP 005-standarden följs eller inte. Om detta görs beror på om den elektroniska säkerhetsgränsen och sårbarhetsutvärderingen följer standarden eller inte. Om dessa två entiteter följer standarden beror i sin tur på om andra entiteter uppfyller de kriterier som ställs i NERC CIP 005. Kort sagt finns attributen i modellen för att beskriva entiteternas egenskaper och tillstånd så att man kan avgöra om man följer standarden eller inte.

.



Figur 3. En abstrakt modell av elektroniskt gränssnittsskydd i enlighet med NERC CIP 005, utökad med tillhörande attribut.

Exakt vilka attribut som påverkar varandra (och i slutändan om man lever upp till kraven eller inte) beskrivs i detalj med **attributsrelationer**. Dessa pilar (se de gröna pilarna i Figur 4 som går till och från attributen) innebär att attributet vid pilens spets påverkas av det vid dess bas. Hur denna påverkan sker specificeras genom sannolikhetstabeller som den i dialogfönstret i Figur 4. Den formalism som används här för att beräkna variablers påverkan på varandra på ett statistiskt sätt är en form Bayesiansk matematik kallad influensdiagram.



Figur 4. En abstrakt modell av elektroniskt gränssnittsskydd i enlighet med NERC CIP 005, utökad med tillhörande attribut samt attributsrelationer. Dialogrutan visar hur de sannolikhetstabeller som matematiskt definierar attributsrelationerna sätts.

Attributsrelationerna relateras dessutom till en relation mellan entiteter (grafiskt illustrerat med streck mellan de olika relationerna. T.ex. påverkar attributet ”Compliant” i entiteten ”Electronic security perimeter” attributet ”Nerc CIP 005 compliant” i entiteten ”Resposible entity” om, och endast om, denna ”Electronic security perimeter” har relationen ”is governed by” till ”Responsible entity” i den konkreta modellen. Detta är viktigt då det i den konkreta modelleraren behöver identifieras vilka attribut som påverkar vilka, och detta görs baserat på vilka relationer som finns mellan attributens entiteter. Det är ju t.ex. bara de säkerhetsgränssnitt som vår ansvariga enhet faktiskt ansvarar för som är relevanta vid utvärderingen av huruvida man följer standarden eller inte, förstås inte alla existerande säkerhetsgränssnitt.

Sammanfattningsvis används alltså den abstrakta modelleraren till att beskriva generella teorier i en grafisk modellform. Ett annat sätt att uttrycka saken på är att den abstrakta modellen definierar det modelleringsspråk i vilket vi sedan skall uttrycka våra faktiska scenarion samt hur beräkningen av dessa scenarions egenskaper görs.

Vidare kan nämnas att arbetet med att skapa abstrakta modeller är typiskt forskningsarbete och det är alltså på detta sätt som ny teoretisk kunskap

matas in i verktyget. Således är också den abstrakta modelleraren främst ämnad att användas av universitet och potentiellt en utvärderingsledare eller liknande.

Den konkreta modelleraren

Den abstrakta modellen bestämmer alltså vad som skall modelleras i den konkreta modellen. Har man t.ex. i den abstrakta modellen inte med entiteten ”dokument”, kan man inte heller modellera alla de dokument som finns ute i verkligheten i den konkreta modellen. Med anledning av detta är det första man gör i den konkreta modelleraren att välja vilken abstrakt modell (det kan ju potentiellt finnas många som har olika syften) man vill basera sig på – annars kan man inte modellera någonting alls. Dvs. först bestämmer man sig för vad som ska analyseras, i detta fall huruvida NERC CIP 005 uppfylls.

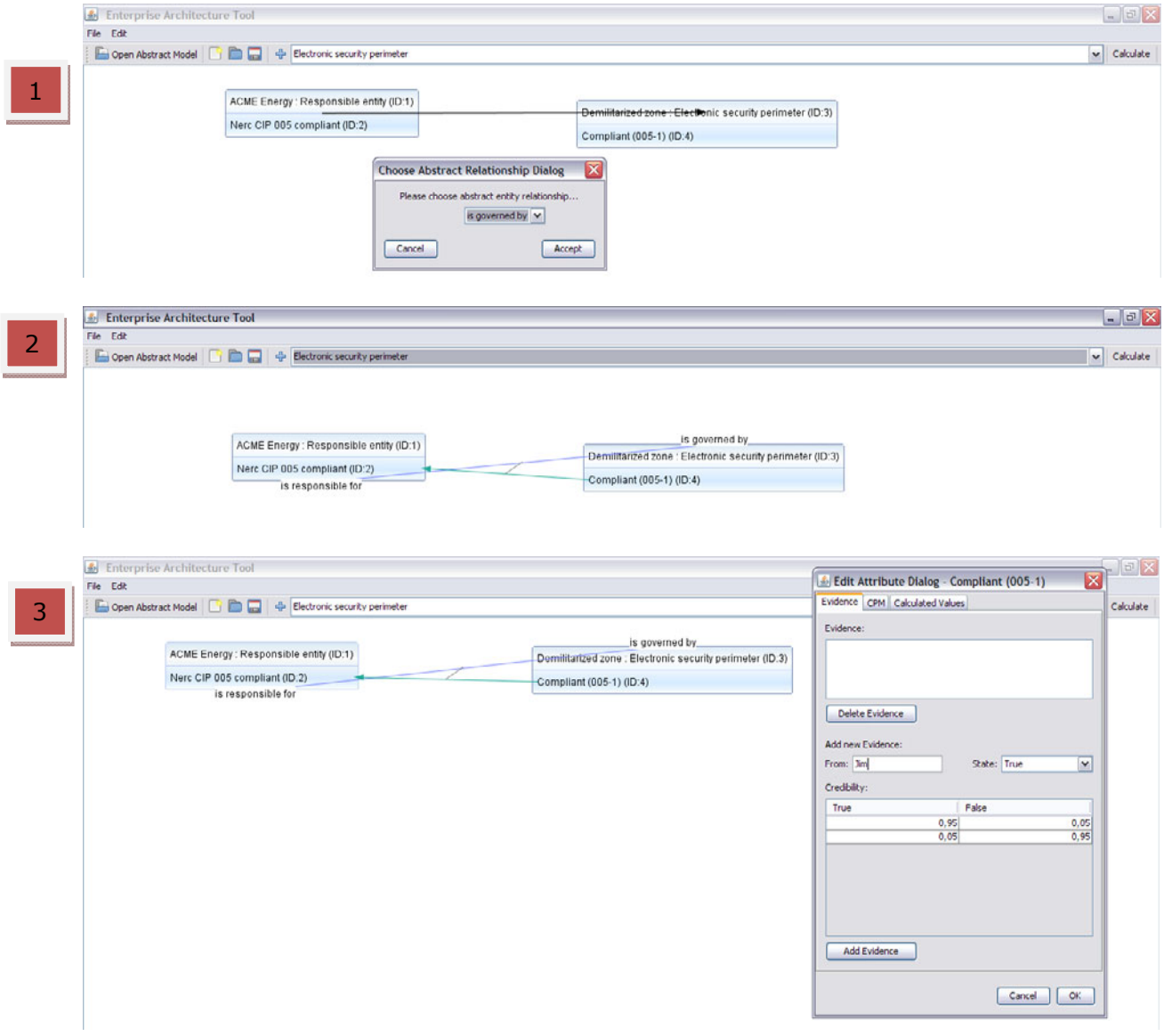
När detta är gjort finns möjligheten att skapa en modell som innehåller de entiteter som finns beskrivna i den abstrakta modellen, tillsammans med relationerna mellan dem. I Figur 5 har den abstrakta modell som visats ovan laddats in och man kan således välja på att modellera de entiteter som återfinns i den abstrakta modellen.

Figur 5. Den abstrakta modellen som skall användas för den konkreta modellen anges. I detta fall den abstrakta modellen av NERC CIP 005 som beskrivits ovan. I menyn återfinns entiteterna från den abstrakta modellen.

Att bygga upp en konkret modell över ett systemscenario görs sedan ”grafiskt” genom att lägga till entiteter (via högerklick eller att klicka i verktygsfältet), namnge dessa och (med muspekaren) dra relationer mellan dem. Man skapar på detta sätt en modell som representerar den nuvarande arkitekturen eller en potentiell framtida arkitektur.

I vårt exempel skall vi modellera företaget ACME Energy och ta reda på huruvida de uppfyller kraven i NERC CIP 005 eller inte. Figur 6 illustrerar hur en modell av ACME byggs upp steg för steg med entiteter och relationer samt värden/tillstånd på attributen i entiteterna. I Figur 6 del 1, har två entiteter lagts till sedan tidigare; ACME Energy som är av typen ”Responsible Entity” och en demilitariserad zon som är ett elektroniskt säkerhetsgränssnitt. När man nu försöker koppla samman de två entiteterna frågar verktyget vilken typ av relation de har till varandra och man kan då välja på de i den abstrakta modellen tillåtna relationerna. I detta fall kan man endast välja på att säkerhetsgränssnittet sköts av ACME. I och med att de två entiteterna kopplats samman visar verktyget att de två attributen också har en relation enligt den abstrakta modellen, se Figur 6 del 2. Huruvida hela ACME är ”compliant” beror alltså på om gränssnittet är ”compliant”.

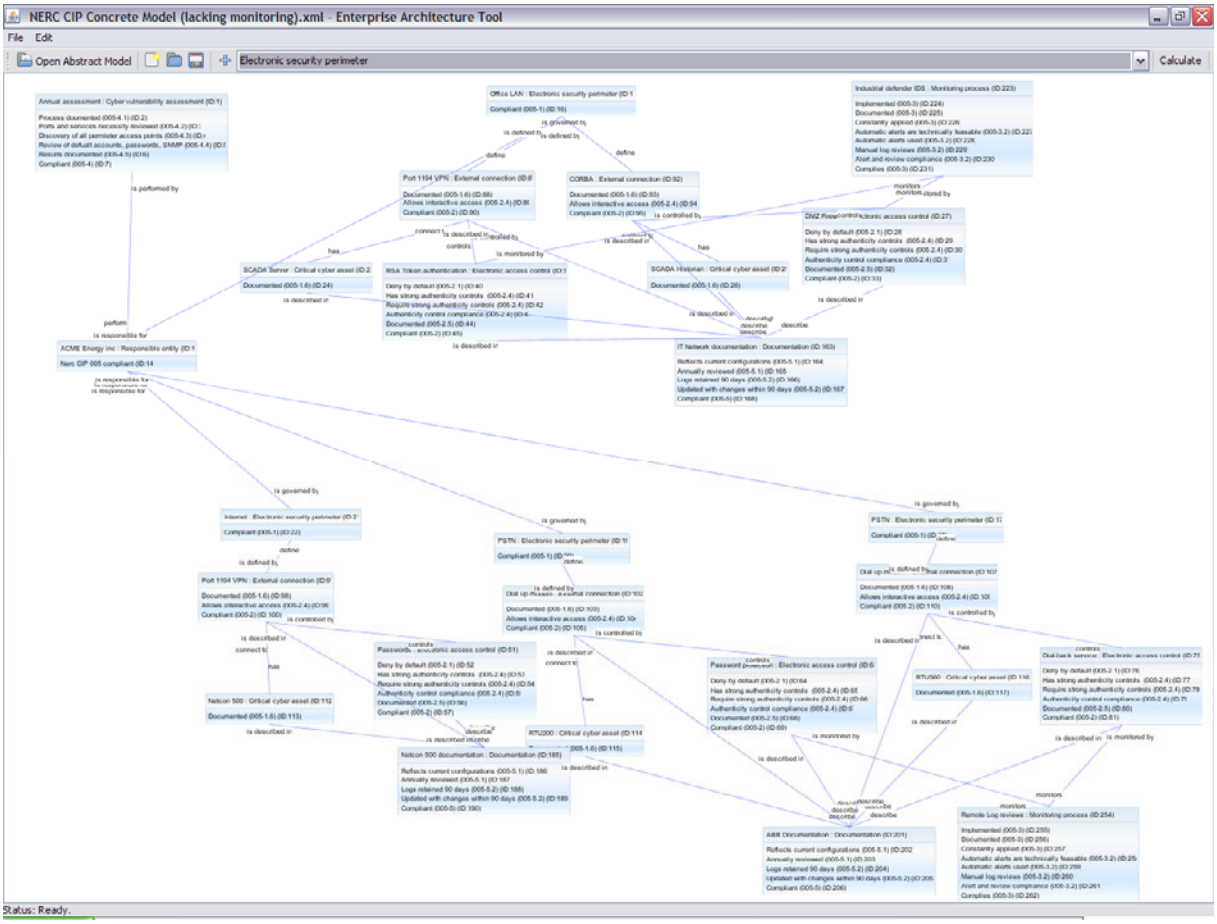
Slutligen anges värdena på attributen i Figur 6 del 3. När man anger attributvärden måste man också ange varifrån man fått uppgiften – vilket är beviset för att vi sätter detta värde? I exemplet anger vi att källan ”Jim” har tillhandahållit information om att den elektroniska behörighetskontrollen för ACMEs demilitariserade zon verkligen är ”Compliant” (dvs att attributet har har värdet ”true”). Man kan här om man vill också ange hur tillförlitliga bevis man har. Huruvida det är sannolikt att värdet faktiskt är ”true” beror ju på vilken roll Jim har i företaget och vad han i och med detta har kompetens att uttala sig om; är han VD, vaktmästare eller kommunikationsnätverkstekniker? I detta fall tror vi att det är 95% sannolikt att Jim har rätt i sin utsago.



Figur 6. Stegvis modellering av det fiktiva företaget ”ACME Energy”.

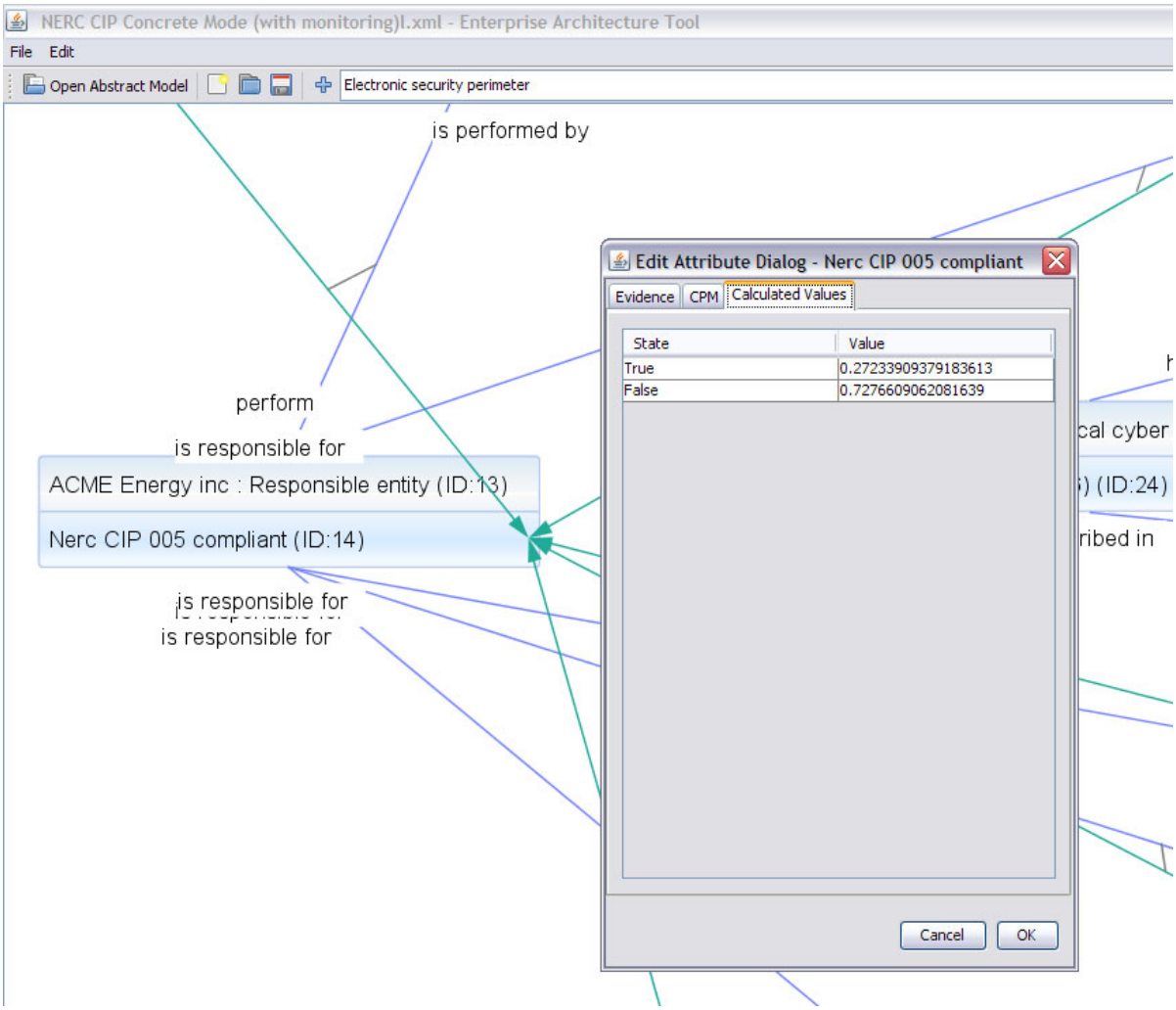
Man fortsätter sedan att modellera sitt scenario på detta sätt till dess att man fått med alla aspekter av det som den abstrakta modellen tillåter och föreskriver. Ett exempel på ett mer omfattande arkitekturscenario återfinns i Figur 7. I detta scenario ansvarar vår ansvariga entitet ”ACME Energy” för fyra stycken elektroniska säkerhetsgränser, två kopplingar till telefonnätet (PSTN), ett till Internet och ett till kontors-LANet. Dessa gränssnitt är i sin tur definierade av fem stycken externa kopplingar med namn som: ”Port 1194 VPN”, ”Dial up modem” och ”CORBA”.

I scenariot finns ytterligare en mängd saker modellerade. Vi hittar exempelvis SCADA-systemkomponenter och RTU:er (Remote Terminal Unit), vilka är den känsliga utrustningen ACME Energy försöker hålla skyddad mot intrång, samt autentiseringsmekanismer för de olika säkerhetsgränssnitt med tillhörande övervakningsmekanismer för detta samt tillhörande dokumentation av utrustningen. Vidare finns också den manuella process som en gång om året går igenom och utvärderar systemkonfigurationen i företaget. Slutligen har varje attribut på varje entitet i modellen har ett värde som fåtts från ett bevis. (Vid avsaknad av bevis anges detta som en jämn fördelning över attributets all möjliga tillstånd, vilket alltså motsvarar full osäkerhet på värdet.)



Figur 7. En fullskalig modell av det fiktiva (och förenklade) företaget ”ACME Energy”.

Givet en modell som den i Figur 7, med bevis på attributen kan en sannolikhet beräknas för att ”ACME Energy” följer alla de krav som finns stipulerade i NERC CIP 005. Detta görs probabilistiskt utifrån alla attributs tillstånd (som alltså angetts här i den konkreta modellen), de attributsrelationer som finns och de sannolikhetstabeller som finns specificerade (vilka angetts i den abstrakta modellen av en forskare eller utvärderingsledare). I Figur 8 kan man se att beräkningen ger att det är 27% sannolikhet att ”ACME Energy” i vårt exempel följer standarden.



Figur 8. Utvärderingens resultat: sannolikhet att ”ACME Energy” följer kraven NERC CIP 005 är 27%.

Även om detta förstås är ett helt fiktivt värde är det lämpligt att här nämna något om anledningarna till detta värde och hur man kan åtgärda det. Att sannolikheten för att man följer standarden är så låg beror på två saker primärt: dels är det så att standarden förelägger att allt som föreskrivs måste vara på plats för att man skall uppfylla kraven - och med en stor mängd parametrar är sannolikheten stor att någon av dem inte uppfyller kraven, dels finns en hel del osäkerheter angivna i de insamlade bevisen. Det man kan göra åt detta är förstås att identifiera vilka de ”svaga parametrarna” är och

förbättra dessa. (Det man kan göra i verktyget är att ”simulera” hur förbättringar av olika parametrar skulle påverka resultatet.)

Det är också viktigt att poängtera att denna utvärdering inte säger något om det faktiska förhållandet huruvida ACME Energy uppfyller NERC CIP 005 eller inte, bara sannolikheten för detta. Vill vi veta exakt hur saken ligger till har vi inget annat val än att samla in bevis som är helt utan osäkerheter (vilket i alla praktiska sammanhang är mycket kostsamt). Men för att bli säkrare på sitt resultat måste man alltså spendera mer resurser på att få in säkrare bevis på värdena i attributen i modellen – detta oavsett om resultatet i slutändan är att man uppfyller kraven i standarden eller inte.

4.1.2 Tekniska plattformskomponenter

Tekniskt sett är verktyget skrivet i Java. Som utvecklingsmiljö används Netbeans IDE 6.1 [5]. För hantering av versioner i programvaran används verktyget Subversion [8]. De abstrakta och konkreta modeller som skapas i verktyget sparas i eXtendible Markup Language (XML)-format [2]. För att omvandla XML till Java och vice versa används Castor [1]. För grafiken har Netbeans grafikmodul använts. Slutligen har de Smile använts för att göra de statistiska beräkningarna [7].

4.2 Instruktionsmanual och publikationer

Den tekniska dokumentation om verktyget som projektet tagit fram redovisas nedan. Alla dokument återfinns som bilagor till denna rapport (samlade i en zip-fil):

- Instruktionsmanual. Instruktionsmanualen beskriver hur verktyget kan användas och gör verktyget mer tillgängligt för industriella användare. ***Bilaga 1.***
- Utbildningspaket. Utbildningspaketet beskriver bakgrunden kring projektet samt ett antal introducerande övningar för verktyget. ***Bilaga 2.***
- Forskaningsartiklar
    - Pontus Johnson, Erik Johansson, Teodor Sommestad, and Johan Ullberg. A Tool for Enterprise Architecture Analysis. In Proceedings of the 11th IEEE International Enterprise Computing Conference (EDOC 2007), oktober 2007. ***Bilaga 3.***
    - Mathias Ekstedt, Ulrik Franke, Pontus Johnson, Robert Lagerström, Teodor Sommestad, Johan Ullberg, and Markus Buschle. A Tool for Enterprise Architecture Analysis of Maintainability. Proc. 13th European Conference on Software Maintenance and Reengineering, mars 2009. ***Bilaga 4.***
- Examensarbeten
    - Tanja Lehtola. Enterprise Architecture Analysis - Development of a Java based Assessment tool. Kungliga Tekniska högskolan, maj 2008. ***Bilaga 5.***

- Ubaldo Pescatore. A Java-based assessment tool for enterprise architecture analysis. Kungliga Tekniska högskolan och University of Sannio Italien, 2008. ***Bilaga 6.***

Utöver dessa publikationer är två examensarbeten pågående som kommer att rendera i följande rapporter under 2009:

- Daniel Feller, Torsten Derlat, and Markus Buschle. Probabilistic Relational Models and Enterprise Architecture – Implementation of the Abstract and Concrete Modeler. Kungliga Tekniska högskolan och Technical University of Berlin (TUB), Tyskland.
- Ann-Cathrin Dykström. A Tool for Enterprise Architecture Analysis - Development of a Java NetBeans based Graphical Assessment tool. Kungliga Tekniska högskolan

Utöver denna dokumentation finns förstås också källkoden till verktyget med tillhörande koddokumentation.

4.3 Övriga resultat

Utöver de ovan beskrivna primära resultaten som var en del av målsättningen med projektet har ett antal viktiga sekundära resultat producerats i projektet.

- En plattform för vidare forskningsprojekt. I och med valet av att göra ett generellt verktyg har detta också blivit relevant för andra forskare och projekt. Verktyget har nu god potential att kunna anpassas för att användas som stöd även för andra typer av systemanalyser. (En allmän workshop om verktyget hölls den 23 oktober 2008 på KTH, för vidare info se http://www.ics.ee.kth.se/eaday)
- En fungerande och återanvändbar projektplattform. Mycket erfarenhet om hur denna typ av utvecklingsprojekt bedrivs på ett effektivt sätt har kommit ur projektet. Framförallt finns nu:
  - en etablerad projektorganisation. Detta projekt är nu pågående och behöver inte ägna tid och resurser med att få till en bra arbetsfördelning och arbetsorganisation med tillhörande projektverktyg (t ex en projekt-wiki).
  - en etablerad utvecklingsmiljö. Att förstå hur programvaru-utvecklingsmiljön fungerar är i sig resurskrävande. I projektet har nu en god kunskap om utvecklingsmiljön och andra tredjepartsprodukter skapats.
- En genomförd NERC-CIP analys hos E.On.
- Projektet har också bidragit med en hel del nytta internt till forskningen på KTH/ICS.
  - Förbättrad metodik. Som en konsekvens av detta projekt har det bedömts nödvändigt att utveckla och hålla en doktorandkurs i Bayesiansk statistik på avdelningen för Industriella informations- och styrsystem.

- Verktyget kommer på sikt kunna vara en plattform för många andra forskningsprojekt på så sätt att resultaten från forskningen kan modelleras i det framtagna verktyget (om det anpassas något).
- Utökat samarbete med tekniska universitetet i Berlin. Ett av examensarbetena har utförts a studenter tekniska universitetet i Berlin. I och med detta har också starkare band knutits till motsvarande forskargrupp där.

5 Framtida arbete

Metoder för informationssäkerhetsutvärdering är sedan tidigare utvecklade inom ramen för forskningen på avdelningen för Industriella informations- och styrsystem. Metoderna är dels baserade på en typ av probabilistiska attackträd; en vidareutveckling av felträdsanalys, dels på informations-systemmodellering.

Detta projekt har möjliggjort utvecklingen av ett programvarubaserat verktygsstöd för dessa metoder. Verktyget behöver emellertid vidareutvecklas i framförallt i två avseenden. För det första behöver användbarheten förbättras för att förenkla användningen för praktiker. Detta innebär att den grafiska presentationen av det symbolspråk som används i styrsystemsmodelleringen skall uppdateras och göra mer naturligt samt att menysystemet och wizards för att genomföra göra analysen skall förenklas. För det andra behöver verktyget skräddarsys mer mot SCADA-system. Den befintliga versionen är relativt generell till sin karaktär. Verktyget behöver utvecklas för att tillåta mer fler men även mer detaljerade utvärderingar anpassade till styrsystem.

Ett fortsatt projekt är planerat att genomföras iterativt, där verktyget utvecklas till en ny release, varpå det testas ute hos intressentföretag. De erfarenheter som kan tillgodogöras från tillämpningen används för att förbättra verktygsstödet. Samtidigt kan också verktyget anpassas till de rutiner för riskbedömning och hantering av informationssäkerhet som redan existerar hos eldistributionsföretagen. Bedömningen är att två alternativt tre tillämpningar behöver genomföras innan verktygsstödet kan anses färdigt för allmänt bruk, och projektet kan avslutas.

Det fortsatta arbetet kommer i huvudsak att ske vid avdelningen för Industriella informations- och styrsystem. Precis som hittills är arbetet planerat att utföras huvudsakligen av seniora forskare och doktorander. Examensarbetare kommer att involveras i delar av implementationen. Examensarbeten kommer även att bedrivas med företag inom kraftbranschen för att anpassa verktyget och dess användande praktiskt.

Detta fortsatta arbete kan starta hösten 2008 och arbetet bedöms motsvara en senior halvtidstjänst löpande över två och ett halvt kalenderår vilket innebär att avslut i så fall beräknas till december 2010.

6 Referenser

[1] Castor is an Open Source data binding framework for Java, http://www.castor.org/

[2] Extensible Markup Language (XML), http://www.w3.org/XML/

[3] Jensen, F., "*Bayesian Networks and Decision Graphs*", Springer-Verlag, 2001

[4] NERC CIP-002-1 till CIP-009-1 Standard. Utgiven av North American Reliability Council (NERC), U.S.A. http://www.nerc.com/~filez/standards/Cyber-Security-Permanent.html

[5] Netbeans IDE 6.1, The IDE runs on Windows, Linux, Mac OS X and Solaris. NetBeans IDE is open-source and free, http://www.netbeans.org/

[6] Pearl, J., "*Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference*", Morgan Kaufmann, 1988.

[7] SMILE (Structural Modeling, Inference, and Learning Engine), http://genie.sis.pitt.edu/

[8] Subversion is an open source version control system, http://subversion.tigris.org/

Det pågår för övrigt ett omfattande internationellt arbete kring säkerhet i digitala kontrollsystem. Nedan listas några utvalda böcker och några av de etablerade webbsidorna inom området som kan vara värde fulla att titta närmare på.

[9] Allen, R., R. Douence, D. Garlan, "Specifying and Analyzing Dynamic Software Architectures" *Proceedings of the 1998 Conference on Fundamental Approaches to Software Engineering*, 1998

[10] Boyer, S. A. (2004) SCADA: supervisory control and data acquisition. The Instrumentation, systems, and automation society (ISA), Research Triangle Park, N.C.

[11] Cegrell, T. & Sandberg, U. (1994) Industriella styrsystem. SIFU förlag, Borås.

[12] Centre for the Protection of National Infrastructure (CPNI), U.K. http://www.cpni.gov.uk/ProtectingYourAssets/ElectronicSecurity/scada.aspx

[13] Clements, P., R. Kazman, M. Klein, "*Evaluating Software Architectures: Methods and Case Studies*", Addison-Wesley, 2001

[14] Department of Homeland Security (DHS), US-CERT, Control Systems Security Program, U.S.A. http://www.us-cert.gov/control_systems/

[15] DoD Architecture Framework Working Group, "*DoD Architecture Framework*" Version 1.0, 2003

[16] Druzdzel MJ and L.C. van der Gaag, "Building probabilistic networks: where do the numbers come from?" *IEEE Trans Knowledge Data Eng* 2000;12:481–6.

[17] Druzdzel, M.J. and L.C. van der Gaag, "Elicitation of Probabilities for Belief Networks: Combining Qualitative and Quantitative Information," *Proc. 11th Conf. Uncertainty in Artificial Intelligence*, pp. 141-148, 1995

[18] Gacek, C., "*Detecting Architectural Mismatch During System Composition*", PhD. Thesis, University of Southern California, 1998

[19] Hughes, J., *The Integrated Energy and Communication Systems Architecture*, Electric Power Research Institute, 2004

[20] Johansson, E. and P. Johnson, "Assessment of Enterprise Information Security – Estimating the Credibility of the Results", *Proceedings of the 9th IEEE international Annual Enterprise Distributed Object Computing Conference*, The Netherlands, 2005.

[21] Johansson, E., H. Christiansson, R. Andersson, G. Björkman and A. Vidström "Aspekter på antagonistiska hot mot SCADA-system i samhällsviktiga verksamheter", Krisberedskapsmyndigheten, Stockholm, 2007. www.krisberedskapsmyndigheten.se/upload/SCADA_studie%20_070903.pdf

[22] Johansson, E., M. Ekstedt, P. Johnson, "Assessment of Enterprise Information Security – The Importance of Information Search Cost", *Proceedings of the 39yh IEEE Hawaii International Conference on System Sciences*, Hawaii, 2006

[23] Johnson, P. and M. Ekstedt, *Enterprise Architecture – Models and Analyses for Information Systems Decision Making*, Studentlitteratur, Sweden, 2007

[24] Johnson, P. et. al. "Enterprise Architecture Analysis with Extended Influence Diagrams", *Information Systems Frontiers*, Volume 9, issue 2-3, 2007

[25] Johnson, P., E. Johansson, T. Sommestad, J. Ullberg, "A Tool for Enterprise Architecture Analysis", *Proceedings of the 12th IEEE international Annual Enterprise Distributed Object Computing Conference*, Germany, 2008.

[26] Kjaerulff, U., "Reduction of Computational Complexity in Bayesian Networks through Removal of Weak Dependences," *Proceedings of the 10th Conference on Uncertainty in Artificial Intelligence*, pp. 374-382, 1994

[27] Lagerström, R., P. Johnson, P. Närman, "Extended Influence Diagram Generation", *Proceedings of the third International Conference on Interoperability for Enterprise Software and Applications,* Springer-Verlag Portugal, 2007

[28] Medvidovic, N., D. Rosenblum, R. Taylor, "A Language and Environment for Architecture-Based Software Development and Evolution", *Proceedings of the 21st International Conference on Software Engineering*, 1999

[29] MoDAF, "*Ministry of Defense Architecture Framework*", Version 1.0, 2005

[30] NAF, "*NATO C3 Technical Architecture*", Volume 1-5, Version 7.0, Allied Data Publication 34, 2005

[31] Olesen, K.G. et. al. "A MUNIN Network for the Median NerveÐA Case Study on Loops", *Applied Artificial Intelligence*, vol. 3, pp. 385-404, 1989

[32] OMB – U.S. Office of Management and Budget, "*FEA Consolidated Reference Model Document*", Version 2.1, 2006

[33] OMG, *Unified Modeling Language: Superstructure*, version 2.1.1, February 2007

[34] Process Control Systems Forum (PCSF), U.S.A. https://www.pcsforum.org/

[35] Qualiware, *Qualiware*, http://www.qualiwareinc.com/, accessed May 2007

[36] SCADA Blog (Digital Bond), U.S.A. http://www.digitalbond.com/

[37] Scheer, A.-W., *Business Process Engineering: Reference Models for Industrial Enterprises*, 2nd ed., Springer-Verlag, 1994.

[38] Shaw, W. T. (2006) Cybersecurity for SCADA systems. PennWell Corp., Tulsa.

[39] Srinivas S., "A Generalization of the Noisy-OR Model", *Proceedings of 9th Conference on Uncertainty in Artificial Intelligence,* pp. 208-215, 1993.

[40] Telelogic, *System Architect*, http://www.telelogic.com/products/systemarchitect/, accessed: May 2007.

[41] The Open Group. *The Open Group Architecture Framework*, Version 8, 2005

[42] Troux Technologies, *Metis*, http://www.troux.com/products/, accessed May 2007

[43] Zachman, J., *A framework for information systems architecture,* IBM Systems Journal, 26(3), 1987