

Structuri conceptuale pentru controlul inferenței

Înainte de proiectarea bazei de date trebuie să examinăm aplicația și să determinăm dacă există încălcări potențiale ale securității. Sunt necesare modele semantice de date, precum rețelele semantice și grafurile conceptuale, pentru a modela o aplicație și a efectua raționamente asupra acesteia. Vom analiza utilizarea structurilor conceptuale pentru controlul inferenței.

Anumite tipuri de modele de date semantice, cum ar fi grafurile conceptuale ale lui Sowa (1984), s-au dovedit a fi la fel de puternice ca logica de ordinul întâi. De asemenea, s-a arătat că grafurile conceptuale pot fi extinse în mod natural pentru a trata probleme legate de mod și timp.

Motivația principală pentru utilizarea modelelor semantice de date este următoarea:

1. Utilizarea modelelor semantice de date pentru reprezentarea aplicațiilor este consistentă cu modul în care oamenii percep lumea.
2. Este mai convenabil ca aplicația să fie analizată manual atunci când este reprezentată sub formă de graf (decât ca tabel sau într-un anumit limbaj).
3. O reprezentare a aplicației utilizând modele semantice de date poate fi folosită ca subsistem *front-end* al unui sistem bazat pe programare logică.
4. Strategiile pentru raționament pentru reprezentările bazate pe modele semantice de date sunt suficient de bine dezvoltate.

Utilizarea modelelor semantice de date pentru tratarea problemei inferenței a fost propusă prima dată de Hinke (1988). Acesta a propus utilizarea grafurilor pentru reprezentarea aplicației și a arătat cum poate fi detectată inferența prin traversarea drumurilor alternative între două noduri din graf. Această tehnică permite detectarea inferențelor simple prin proprietatea de tranzitivitate, însă nu este posibilă detectarea celor mai complexe.

Rețele semantice și problema inferenței

Modelele semantice de date sunt interesante pentru că pot fi folosite la reprezentarea unei aplicații multinivel. O astfel de reprezentare poate fi folosită de către SSO pentru a analiza manual aplicația, cu scopul de a asigura că utilizatorii nu pot efectua inferențe neautorizate. Pe de altă parte, putem construi un sistem care procesează cunoștințele folosind strategii care au fost

dezvoltate pentru modele semantice de date și care efectuează automat analize referitoare la securitatea aplicației.

Rețelele semantice sunt modele simple și cu putere de reprezentare a raționamentului.

Rețelele semantice standard nu pot reprezenta aplicațiile multinivel, prin urmare au fost introduse extinderi ale acestora.

Considerăm că o rețea semantică este o colecție de noduri conectate prin muchii. Nodurile reprezintă concepte, entități etc., iar muchiile reprezintă relații între ele.

1. Rețele semantice multinivel

O rețea semantică multinivel (*Multilevel Semantic Net – MSN*) este o rețea semantică ale cărei noduri și muchii sunt clasificate la diferite niveluri de securitate. Figura 2 prezintă câteva rețele semantice multinivel simple. Presupunem că există doar două niveluri de securitate, Unclassified și Secret. Observațiile pot fi extinse spre a include niveluri multiple de securitate. Presupunem că liniile și formele îngroșate se află pe nivelul Secret.

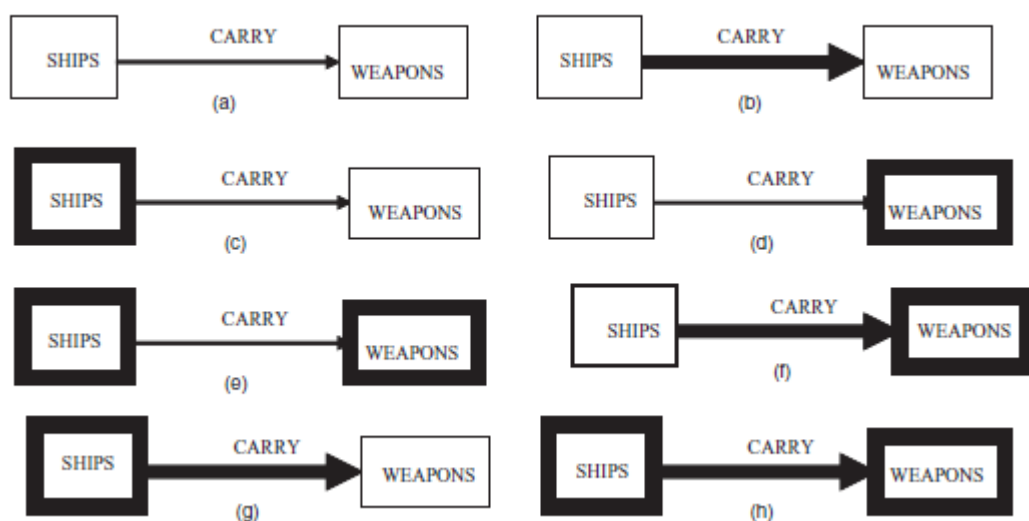


Figura 1. Rețele semantice multinivel

În figura 1a), este reprezentat faptul că navele transportă arme, iar această informație este Unclassified.

În figura 1b), navele și armele sunt Unclassified, însă faptul că navele transportă arme este Secret.

În figura 1c), utilizatorii Unclassified știu că o entitate transportă arme, însă nu cunosc faptul că navele realizează acest transport. În 1d), utilizatorii știu că navele transportă ceva, însă nu știu că transportă arme. În 1e) știu că este realizat un transport, dar nu cunosc transportatorul și obiectele. În 1f), utilizatorii cunosc informații despre nave însă nu cunosc nimic despre arme. Situația este inversată în figura 1g), iar în figura 1h) nimic nu este vizibil utilizatorilor Unclassified.

Este necesar să determinăm dacă toate muchiile descrise în figura 1) sunt permise. De exemplu, poate avea sens să clasificăm o muchie la un nivel care domină nivelurile nodurilor asociate muchiei (nivelul relației „transportă” trebuie să domine nivelurile corespunzătoare armelor și navelor).

Figura 2 prezintă o rețea semantică multinivel mai elaborată. Interpretarea din perspectiva Unclassified a acestei figuri este următoarea: Reagan transportă pasageri. Căpitanul său este Smith și are 20 de ani de experiență. Nava era localizată în Marea Mediterană pe 16 iunie 2000, iar destinația era Italia.

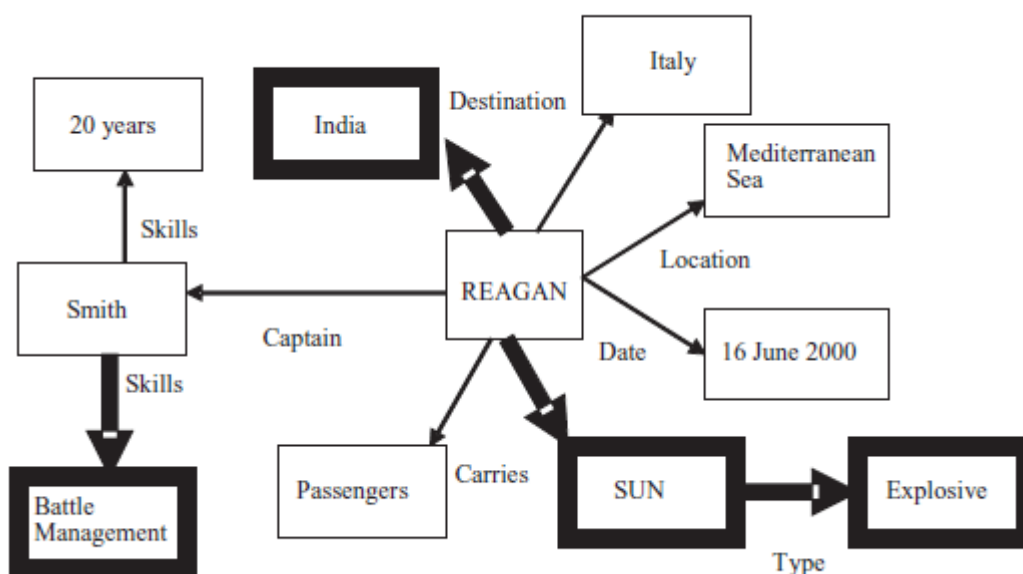


Figura 2. Rețea semantică multinivel complexă

Interpretarea din perspectiva Secret este următoarea: Reagan transportă SUN, care este un exploziv. Căpitanul său este Smith care are experiență de luptă. Nava era localizată în Marea Mediterană pe 16 iunie 2000, iar destinația era India.

Se poate observa că anumite informații sunt poliinstanțiate. **Poliinstanțierea** apare atunci când utilizatorii de la diferite niveluri de securitate vizualizează diferit același concept, entitate,

eveniment sau relație din lumea reală. Acesta este mecanismul utilizat pentru „ascunderea” informației.

Muchiile definite în rețelele semantice, considerate până acum, ilustrează relații specifice. Pe lângă aceste muchii, o rețea semantică are două tipuri de muchii standard: ISA și AKO.

O muchie ISA (*is a*) specifică faptul că un anumit individ aparține unui anumit grup. Figura 3a) arată o muchie ISA în care Reagan este definit ca un tip particular de navă, cum ar fi o navă de luptă.

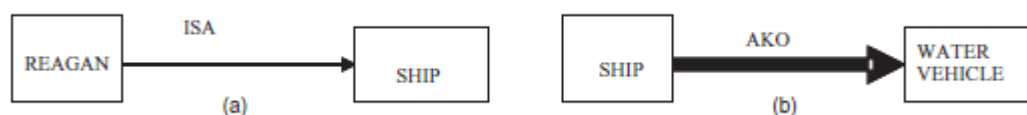


Figura 3. Legături ISA, AKO

O muchie AKO (*a kind of*) definește o submulțime a unei colecții. Figura 3b) definește colecția de nave ca fiind o submulțime a colecției vehiculelor pe apă.

Nu are sens să clasificăm Reagan la nivelul Unclassified și Ship la nivelul Secret, deoarece Reagan este o instanțiere a lui Ship. Clasificând Ship la nivelul Secret, presupunem implicit că orice navă trebuie să fie clasificată cel puțin la nivelul Secret. De asemenea, nu ar avea sens să clasificăm Ship la nivelul Unclassified și Water Vehicle la nivelul Secret, deoarece clasificarea lui Ship la nivelul Unclassified ar presupune implicit că Water Vehicle ar trebui să fie clasificat cel mult la nivelul Unclassified. Clasificarea lui Ship la nivelul Secret presupune implicit că orice Water Vehicle ar trebui să fie clasificat cel puțin la nivelul Secret. Aceasta conduce la un conflict. Prin urmare, se impun următoarele reguli pentru asigurarea consistenței:

A1. Dacă $X \text{ ISA } Y$, atunci $\text{Level}(X) \geq \text{Level}(Y)$

A2. Dacă $X \text{ AKO } Y$, atunci $\text{Level}(X) \geq \text{Level}(Y)$

2. Raționament cu rețele semantice multinivel

Pentru a realiza raționamente avem nevoie de reguli, pe care le vom descrie în continuare.

Cele mai multe aplicații din lumea reală lucrează cu cantități mari de informație, iar o rețea semantică în care să fie captată întreaga informație ar fi extrem de complexă. Avem nevoie de o rețea semantică minimală cu o mulțime puternică de strategii pentru raționament astfel încât

să poată fi deduse alte informații, numite informații implicite. Pentru o aplicație ar trebui ca nivelul informației implicite care poate fi dedus de către un utilizator la nivelul L să fie dominat de L.

Câteva reguli pentru deducerea informației implicite sunt:

A3. Dacă $X \text{ AKO } Y$ și $Y \text{ AKO } Z$ atunci $X \text{ AKO } Z$. Nivelul muchiei AKO de la X la Z este maximul dintre nivelurile muchiilor AKO dintre X, Y și Y, Z.

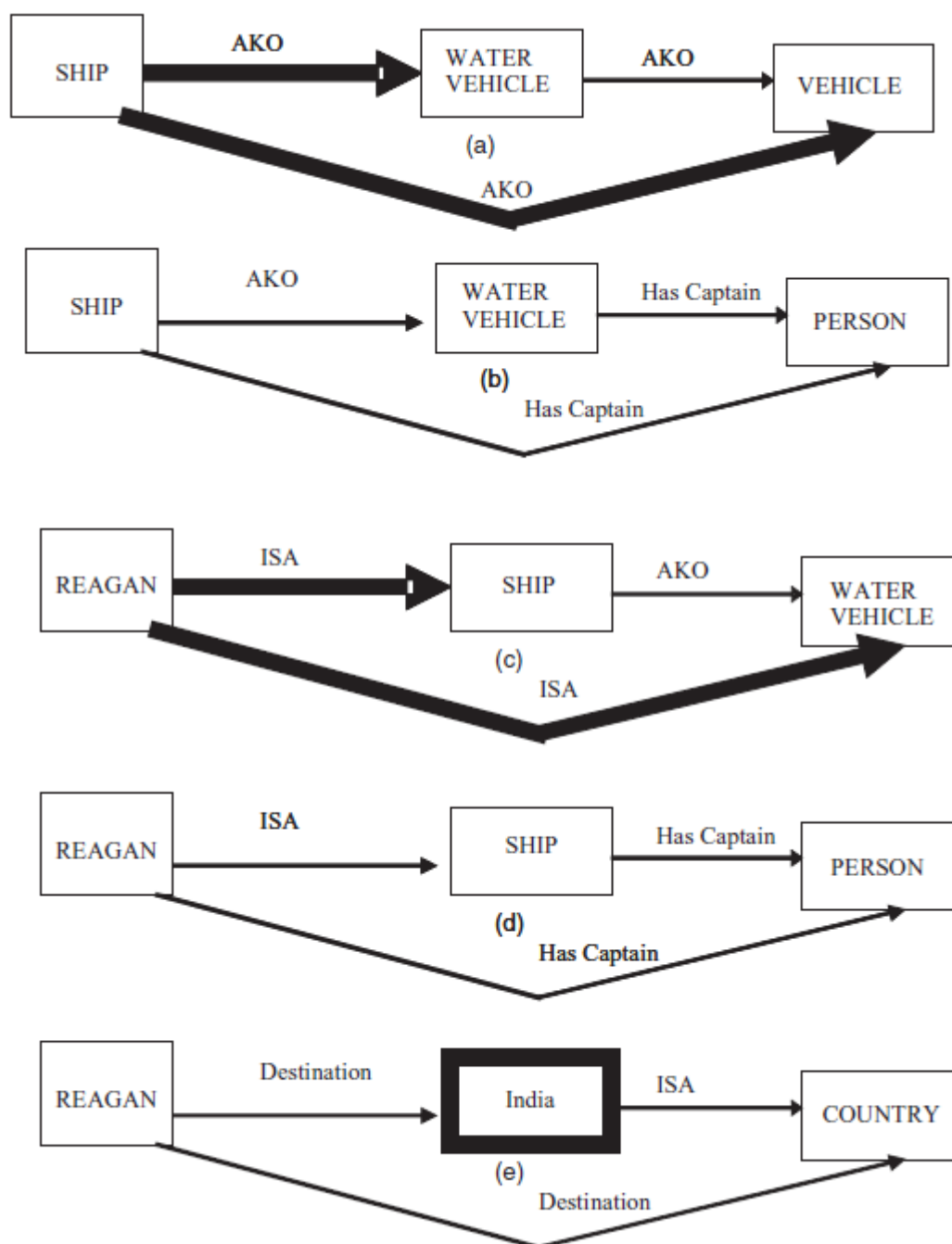


Figura 4. Exemple de reguli

În exemplul din figura 4a) rețeaua semantică conține muchiile „Ship AKO Water Vehicle” și „Water Vehicle AKO Vehicle”. Muchia AKO dintre Ship și Water Vehicle este Secret. Atunci, la nivelul Secret, se poate concluziona că „Ship AKO Vehicle”.

A4. Dacă $X \text{ AKO } Y$ și Y este în relația R cu Z , atunci X se află în relația R cu Z . Nivelul relației R dintre X și Z este egal cu valoarea maximă a nivelurilor asociate muchiei AKO dintre X , Y și relației R între Y , Z .

În figura 4b), rețeaua semantică conține „Ship AKO Water Vehicle” și „Water Vehicle *has captain* Person”. Atunci „Ship *has captain* Person”.

A5. Dacă $X \text{ ISA } Y$ și $Y \text{ AKO } Z$, atunci $X \text{ ISA } Z$. Nivelul muchiei ISA între X , Z este cea egal cu valoarea maximă a nivelurilor muchiei AKO între Y , Z și al muchiei ISA între X , Y .

În figura 4c), „Reagan ISA Ship”. Această muchie este Secret. Dar „Ship AKO Water Vehicle”, prin urmare există o muchie ISA la nivelul Secret între Reagan și Water Vehicle.

A6. Dacă $X \text{ ISA } Y$ și Y se află în relația R cu Z , atunci X se află în relația R cu Z . Nivelul relației R dintre X și Z este egal cu valoarea maximă a nivelurilor asociate muchiei AKO între X , Y și a celui asociat relației R între Y , Z .

În figura 4d), rețeaua semantică are relația „Reagan ISA Ship”. Dar „Ship *has captain* Person”, prin urmare „Reagan *has captain* Person”.

A7. Dacă $X \text{ ISA } Y$ și Z se află în relația R cu X , atunci Z se află în relația R cu Y . Nivelul relației R care există între Z și Y este egal cu valoarea maximă a nivelurilor relației ISA între X , Y și relației R între Z , X .

În figura 4e), rețeaua semantică are relația „India ISA Country”. Destinația lui Reagan este India, prin urmare destinația lui Reagan este o țară.

3. Instrucțiuni condiționale și rețele auxiliare

Instrucțiunile condiționale sunt de forma:

A if B1 and B2 and B3 and ... and Bn, unde B1, B2, ..., Bn sunt antecedente și A este consecința.

Instrucțiunile condiționale reprezintă clauze într-un program logic. O astfel de instrucțiune condițională poate fi reprezentată prin intermediul rețelelor semantice auxiliare.

Considerăm următoarea instrucțiune condițională:

Destinația lui Reagan este India dacă nava este localizată în Marea Mediterană și transportă SUN, care este un exploziv.

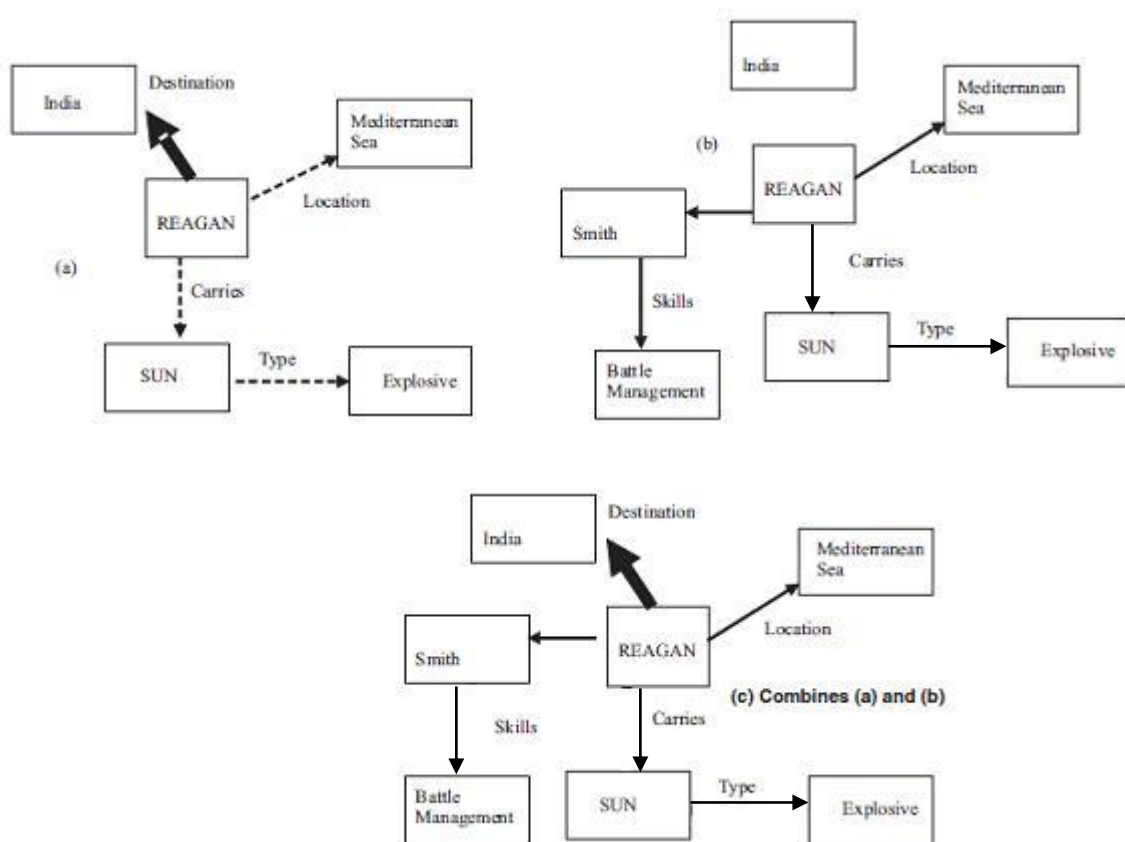


Figura 5. Aplicarea regulii de transfer

Instrucțiunea condițională este reprezentată prin rețeaua auxiliară prezentată în figura 5a). Condițiile sunt reprezentate prin linii punctate, iar concluzia prin linii continue. Regula de transfer va fi aplicată pentru a procesa instrucțiunile condiționale.

A8 (Regula de transfer). Dacă toate liniile punctate din rețeaua auxiliară sunt prezente ca linii continue într-o rețea principală semantică multinivel, iar nivelul fiecărei linii continue a rețelei

principale domină nivelul liniei punctate corespunzătoare din rețeaua auxiliară, atunci linia continuă din rețeaua auxiliară este prezentă ca linie continuă în rețeaua principală. Nivelul de securitate al acestei linii este valoarea maximă a nivelurilor tuturor liniilor din rețeaua auxiliară și tuturor liniilor continue corespunzătoare, care se află deja în rețeaua principală.

Figura 5b) arată că liniile punctate din rețeaua auxiliară apar ca linii continue în rețeaua semantică multinivel. Figura 5c) arată că linia continuă din rețeaua auxiliară este adăugată la rețeaua semantică multinivel la nivelul corespunzător de securitate.

4. Aplicarea constrângerilor de securitate

După cum am afirmat în cursul anterior, constrângerile de securitate sunt reguli care atribuie niveluri de securitate datelor. Vom reprezenta constrângerile de securitate prin „rețele de constrângeri”.

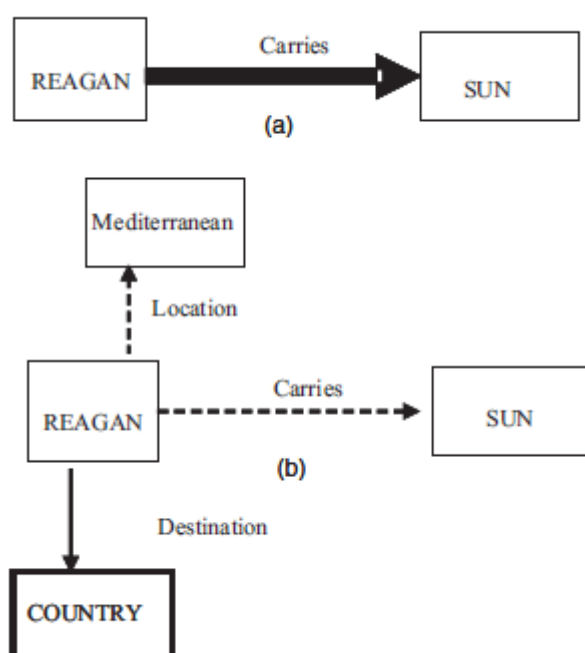


Figura 6. Reprezentarea constrângerilor de securitate

O rețea de constrângeri este o rețea semantică, principală sau auxiliară, care specifică numai constrângeri. Deși rețelele semantice sunt folosite în general pentru a reprezenta informația specifică aplicației, rețelele semantice pentru constrângeri sunt utilizate pentru reprezentarea constrângerilor de securitate astfel încât să poată fi detectată orice nerespectare a securității în aplicație. În mod similar, rețelele semantice auxiliare sunt folosite pentru a deduce

informație implicită, iar constrângerile de securitate reprezentate ca rețele semantice auxiliare sunt utilizate pentru a detecta nerespectări ale securității. Prin urmare, se face diferența între rețelele auxiliare simple și cele referitoare la constrângeri.

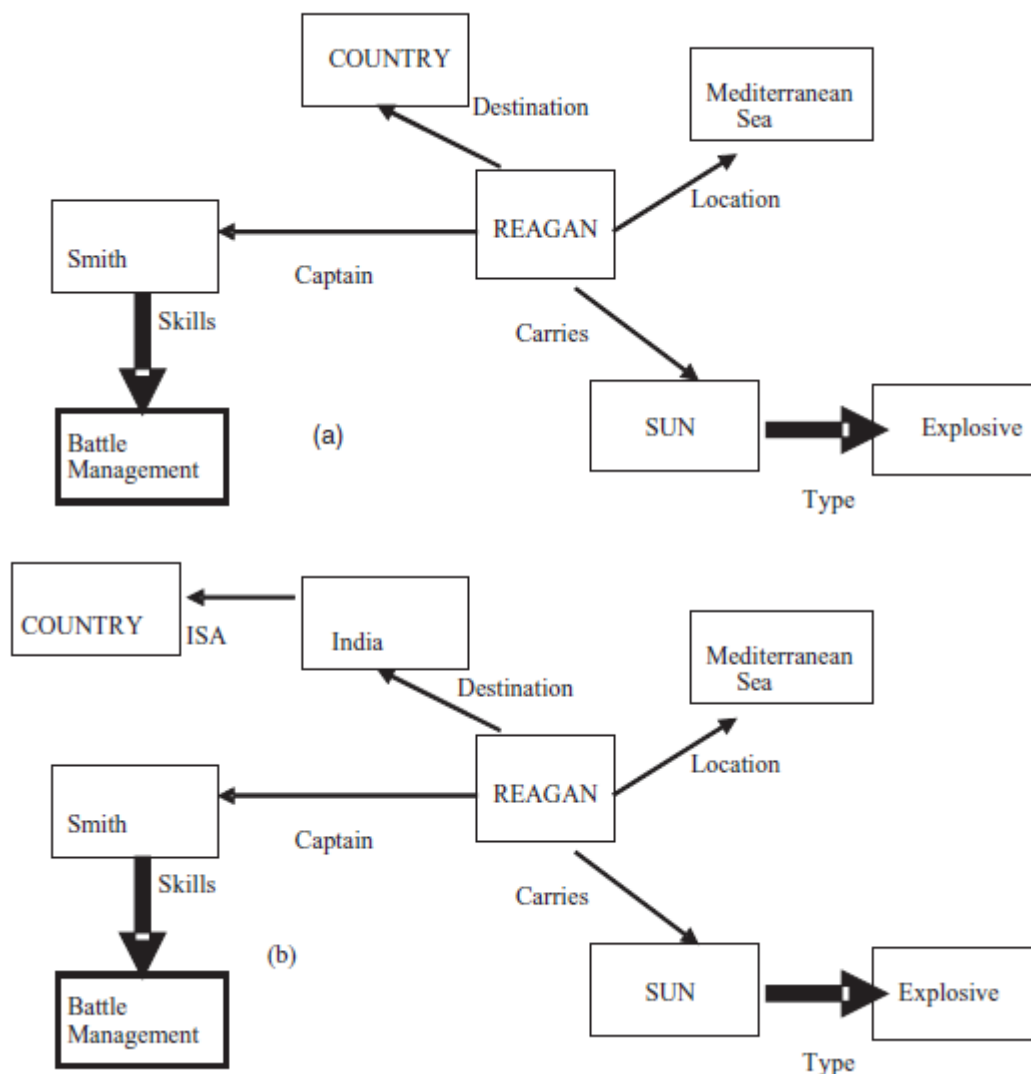


Figura 7. Încălcarea constrângerilor de securitate

Figura 6a) clasifică faptul că Reagan efectuează transporturi la nivelul Secret. Figura 6b) prezintă o constrângere care clasifică țara de destinație a lui Reagan la nivelul Secret, dacă Reagan este localizată în Marea Mediterană și transportă SUN.

Nerespectările de securitate apar (direct sau indirect) dacă rețeaua de constrângeri intră în contradicție cu rețeaua semantică multinivel care reprezintă aplicația (direct sau indirect). Rețeaua semantică din figura 7a) încalcă în mod direct ambele constrângeri din figura 6. În figura 7a), faptul că Reagan transportă ceva nu este Secret, ceea ce încalcă în mod direct

constrângerea din figura 6a). De asemenea, în figura 7a), Reagan este localizată în marea Mediterană și transportă SUN. Țara sa de destinație este Unclassified, ceea ce încalcă în mod direct constrângerea din figura 6b).

Nerespectarea constrângerilor poate avea loc și indirect. Această situație apare atunci când informația implicită intră în contradicție cu constrângerile de securitate. În figura 7b) este arătat modul în care este încălcată constrângerea de securitate din figura 6b) în mod indirect. Aici, Reagan transportă SUN și este localizată în marea Mediterană. Țara sa de destinație, India, este Unclassified. Pe de altă parte, din regula A7, ar rezulta că destinația lui Reagan ar trebui să fie Secret. Prin urmare, constrângerea din figura 6b) este încălcată în mod indirect.