



Arta de a trăi în siguranță.



CONFERINȚA NAȚIONALĂ A A.R.T.S.

**Siguranța și securitatea cetățeanului și a comunității
Aportul tehnicii de securitate**



REZILIENȚA INFRASTRUCTURILOR CRITICE LA NIVELUL COMUNITĂȚILOR LOCALE



Dr. ing. Septimiu CACEU
Director de Proiecte

FUNDATIA EURISC
INSTITUTUL EUROPEAN PENTRU MANAGEMENTUL RISCULUI,
SECURITATII SI COMUNICARII
C.P. 2-111, Bucuresti, Romania
Tf. 021 212 2102 Tf. / Fax : 021 319 3279
E-mail: eurisc@eurisc.org
www.eurisc.org

Definirea Conceptului de Infrastructura și Servicii Critice

Termeni de referință

În sensul Directivei CE 114/2008, din 08 Decembrie 2008:

"Infrastructură Critică" înseamnă un element, un sistem sau o componentă a acestuia, aflat pe teritoriul statelor membre, care este esențial pentru menținerea funcțiilor societale vitale, a sănătății, siguranței, securității, bunăstării sociale sau economice a persoanelor și a căror perturbare sau distrugere ar avea un impact semnificativ într-un stat membru, ca urmare a incapacității de a menține respectivele funcții.

Programul European de Protecție a Infrastructurilor Critice, lansat în Decembrie 2006, menționează următoarea definiție a conceptului:

"Infrastructurile critice se referă la acele obiective, rețele, servicii, active fizice și mijloace informatice care, dacă sunt întrerupte sau distruse, vor avea un impact serios asupra sănătății, siguranței, securității sau a bunăstării economice a cetățenilor sau asupra funcționării efective a actului de guvernare din statele membre".

Programul European pentru Protecția Infrastructurilor Critice (EPCIP), lansat la 12.12.2006 menționează, la nivel European, 11 sectoare și 32 de servicii vitale conexe acestora

Sectorul	Produsul sau serviciul
I. Energetic	1. Producția de petrol și gaze, activitățile de rafinare, tratare și depozitare, inclusiv conductele; 2. Producerea de energie electrică; 3. Transportul de energie electrică, gaze și petrol; 4. Activitățile de distribuție, electricitate, gaz și petrol;
II. Informații și tehnologii de comunicații	5. Sistemele și rețelele de informații; 6. Sistemele de comandă, automatizare și instrumentare; 7. Serviciile de telecomunicații fixe și mobile; 8. Serviciile de radiocomunicații și navigare; 9. Servicii de comunicații prin satelit; 10. Serviciile de radiodifuziune;
III. Alimentare cu apă	11. Furnizarea de apă potabilă; 12. Controlul calității apei; 13. Îndiguirea și controlul cantitativ al apei;
IV. Alimentația	14. Furnizarea de hrană, asigurarea pazei și a securității și siguranței alimentelor;
V. Sănătate	15. Asistența medicală și spitalicească; 16. Medicamente, seruri, vaccinuri, produse farmaceutice; 17. Biolaboratoare și bioagenți;
VI. Financiar	18. Servicii de plăți / structuri aferente; 19. Sisteme financiare guvernamentale;
VII. Apărare, ordine publică și securitate națională	20. Apărarea țării, ordinea publică și securitatea națională; 21. Managementul integrat al frontierelor;
VIII. Administrație	22. Funcționarea guvernului; 23. Forțele armate; 24. Serviciile și administrația; 25. Serviciile de urgență;
IX. Transporturi	26. Transportul rutier; 27. Transportul pe calea ferată; 28. Transportul naval, fluvial, maritim și oceanic; 29. Transportul aerian;
X. Industria chimică și nucleară	30. Producția, procesarea și depozitarea substanțelor chimice și nucleare; 31. Conductele de produse / substanțe chimice periculoase;
XI. Spațiul	32. Traficul aerian.

Definirea Conceptului de Infrastructura Critica și Rezilienta acestora Termeni de referinta

„Comunitatea” este un termen generic care include o metropolă sau oraș, regiune sau județ, de regulă vulnerabile și care pot fi o țintă pentru atacuri directe sau malițioase asupra unor obiective (ex. infrastructuri și servicii critice vitale), care funcționează în acel teritoriu.

Amenințările la siguranța și securitatea unei „comunități” includ pericole de natură tehnică, pericole biologice (epidemii în masă) și pericole teroriste, inclusiv atacuri cibernetice.

La nivelul comunității pot fi analizate diferite scenarii de riscuri și vulnerabilități iar impactul lor evaluat în contextul autorităților administrative locale, a operatorului care gestionează fiecare infrastructură, a obiectivelor economice vizate, precum și al individului în particular și al comunității în ansamblu.

Scenariile analizate permit elaborarea unor politici de dezvoltare locală și de investiții menite să reducă riscurile și să crească reziliența regională, respectiv capacitatea de a reveni, cât mai repede posibil, la nivelul inițial de funcționare a vieții sociale și economice, în situația efectelor negative generate de întreruperi accidentale sau provocate deliberat la diferite infrastructuri și servicii critice vitale pentru comunitățile actuale.

Definirea Conceptului de Reziliencia a Infrastructurilor și serviciilor Critice Termeni de referinta

Reziliența infrastructurilor și a serviciilor critice reprezintă “capacitatea de recuperare rapida a acestora dintr-un incident sau dezastru”.

Aplicarea măsurilor specifice de protecție limitează impactul operațional, reduce riscurile, vulnerabilitățile și efectele în situația unor situații de urgență și dezastre, infrastructurile și serviciile critice fiind capabile să-și reia activitatea într-un interval de timp acceptabil, dependent de vulnerabilitați, amenințări, specificul operațiilor și al serviciilor oferite.

Analiza efectelor posibile și impactul pe plan local, legat de dezastre naturale, urgențe civile, evenimente de natură tehnică și posibil teroriste, presupune realizarea ***unui contract de parteneriat public-privat, care să propună și să realizeze proiecte care să ajute la evaluarea capacității de reziliență a unor servicii și infrastructuri critice vitale pentru cetățeni și activitatea lor zilnică în cadrul “comunității”.***

Obiectivele generale ale proiectelor Parteneriatului Public-Privat

Obiectivele generale ale proiectelor parteneriatului public-privat pentru evaluarea capacității de reziliență a infrastructurilor critice care deserveșc comunitatea, de regulă, sunt următoarele:

- examinarea vulnerabilităților și interdependențelor elementelor de infrastructură critică care funcționează pe teritoriul “comunității”;**
- aprecierea gradului de reziliență la un scenariu de posibil dezastru, la riscuri de natură tehnică sau acțiuni teroriste;**
- evaluarea lipsurilor din capacitatea de reziliență, din gradul de pregătire și capacitatea de răspuns pentru scenariul elaborat, în raport de diferite pericole analizate, ș.a.;**
- evaluarea gradului de pregătire al populației și de răspuns al formațiunilor specializate pentru intervenție;**
- evaluarea impactului economic și social al pericolelor naturale sau create de om asupra sectoarelor care gestionează infrastructurile critice în cauză, datorita interdependenței acestora;**
- stabilirea priorităților pentru investițiile destinate dotării cu echipamente specifice și instruirea personalului, având ca obiectiv creșterea rezilienței, gradul de pregătire și capacitatea de răspuns a cetățenilor și autorităților, în situații critice;**
- elaborarea unei documentații gen „Studiu de caz” care să poată fi utilizată ca un model de abordare și pentru alte comunități din regiuni.**

Evaluarea capacității de reziliență a infrastructurilor critice, gestionate pe plan local

Este esențială participarea activă, conform competențelor fiecărei structuri, a reprezentanților autorităților statului cu responsabilități în domeniu, ***a operatorilor economici care gestionează infrastructuri și servicii critice, a companiilor specializate în domeniul tehnicii de securitate și a securității private, a organizațiilor nonguvernamentale interesate, a reprezentanților mediului academic și massmedia,*** pentru realizarea unor proiecte importante pentru siguranța și securitatea comunităților și a cetățeanului.

Evaluarea capacității de reziliență a infrastructurilor critice, gestionate pe plan local și regional, necesită planificarea și realizarea următoarelor capitole și elemente de bază:

1). Analiza infrastructurilor și a serviciilor critice care deservește comunitatea, având ca obiective:

- stabilirea necesarului de date legate de infrastructurile critice analizate, a metodologiei pentru colectarea de date, circuitul informațiilor și formatul raportului final;
- caracteristicile tehnice și vulnerabilităților ale infrastructurilor critice de asigurare cu energie electrică, termică, produse petroliere, apă, transport, servicii de urgențe, medicale, de procesare și distribuție hrană, de comunicații, etc.;
- evaluarea amenințărilor asupra "comunității", incluzând evenimente naturale extreme, incidente tehnologice și potențial teroriste;
- competențele partenerilor de proiect și relaționarea cu reprezentanții consiliilor de administrație ale obiectivelor analizate;
- modul de acces și utilizare a datelor necesare studiului, stocarea și securitatea acestora precum și cerințele de utilizare a datelor geografice spațiale (GIS).

Analiza interdependenței infrastructurilor și serviciilor critice comunitare și regionale

2). Analiza interdependenței infrastructurilor și serviciilor critice comunitare și regionale, care va avea ca obiective:

- identificarea interdependențelor infrastructurilor și serviciilor critice vitale;
- examinarea impactului unor căderi în cascadă a infrastructurilor și serviciilor critice;
- identificarea metodelor optime de a izola sau limita posibile căderi în cascadă a infrastructurilor și a unor servicii vitale cetățeanului, comunității și pe plan național.

Vor fi luate in considerare urmatoarele elemente:

- Instalații și rețele din sectorul energetic (electricitate, petrol, gaze, agent termic, etc.);
- Infrastructura de comunicații locale, massmedia, rețelele metropolitane de date și acces la Internet, etc.;
- Sectorul financiar-bancar local și cel național;
- Sectorul de prim ajutor, îngrijire a sănătății și serviciile medicale de urgență;
- Sectorul alimentar (producție, procesare, depozitare-distribuție, control sanitar – veterinar)
- Aprovizionarea cu apă potabilă (surse de apă, tratare și rețele de distribuție);
- Evacuare și tratare ape uzate și resturi menajere;
- Transporturile locale, regionale și naționale în zona de reședință (rețele de transport aeriene, terestre și feroviare, sistemele aferente de control trafic, etc.);
- Producția, depozitarea și transportul produselor (materialelor) periculoase (ex: chimice, biologice, radiologice și deșeuri nucleare etc.);
- Buna guvernare, administrare și coordonare pe plan local și regional a serviciilor vitale comunității (administrația locală, poliție, serviciile comunitare, etc.);
- Cultura de securitate privind protecția obiectivelor critice și modul de acțiune în situații de urgență, rețeaua de informare a populației, sistemele de securitate, monitorizare și alarmare pe plan local, etc.).

Interacțiunea dintre societatea civilă, autoritățile locale și structurile centrale

3). Analiza interacțiunii dintre societatea civilă, autoritățile locale și reprezentanții structurilor centrale, va avea ca obiective:

- ☒ dezvoltarea unor norme și variante de acțiune, pentru intervenție la dezastre pe plan local luând în considerare resursele civile și specializate ale statului, existente în zonă;
- ☒ stabilirea unor protocoale pentru un parteneriat public-privat viabil, de colaborare și completarea la nevoie cu personal calificat, acțiuni sau mijloace tehnice de intervenție specifice;
- ☒ stabilirea, unor valori reale și acceptabile pentru fiecare operațiune, serviciu sau resurse materiale utilizate, în vederea decontărilor și recuperării costului acțiunilor de intervenție executate în caz de dezastru.

4). Elaborarea unor aplicații informatice de modelare și simulare a funcționării și interdependențelor Infrastructurilor critice locale cu cele regionale și naționale, având ca obiective:

- ☒ modelarea și simularea funcționării optime a sistemelor de infrastructură care deservește comunitățile locale (comunicații, energie, transport, apă etc.);
- ☒ validarea modelării realizate, în raport cu scopul propus;
- ☒ validarea și rularea modelelor pentru a evalua impactul asupra infrastructurilor analizate, inclusiv pentru căderi în cascadă, în raport de scopul propus și scenariul pregătit pentru studiu;
- ☒ utilizarea datelor de ieșire și a concluziilor rezultate pentru planificarea și bugetarea măsurilor necesare de protecție, reziliență, intervenție cu forțe și mijloace specializate, precum și elaborarea de exerciții de pregătire a populației pentru acțiuni de intervenție în caz de necesitate.

Analiza consecințelor economice și sociale ale intreruperii serviciilor vitale comunității

5). Analiza consecințelor economice și sociale ale intreruperii serviciilor furnizate de către infrastructurile critice vitale și impactul dezastrelor produse, va avea ca obiective:

- definirea și estimarea, onsecințelor economice și sociale a scenariului elaborat;**
- definirea și estimarea efectelor scenariilor elaborate asupra bugetelor locale, și regionale;**
- estimarea costurilor, beneficiilor și riscurilor *activităților de protecție, intervenție și refacere după dezastru*, desfășurate de către administrația publică locală, operatorii de stat sau privați de infrastructuri și servicii critice și alte structuri specializate ale statului.**

6). Analiza politicilor și strategiilor pentru "Reziliență locală și regională", va avea ca obiective:

- evaluarea riscurilor, costurilor, beneficiilor și a schimbărilor asociate unor noi strategii necesare pentru a îmbunătăți reziliența infrastructurilor și serviciilor critice la nivel local și regional;**
- identificarea "punctelor de strangulare" și a discontinuităților în procesul de elaborare și luare a deciziilor în beneficiul cetățeanului, la nivelul autorităților locale, sectorul public subordonat cât și cel privat ,**
- propunerea unor mecanisme de decizie administrativă și elaborare de normative pentru măsurile considerate prioritare pe plan local și regional;**
- stabilirea nevoilor, competențelor și procedurilor de colaborare și cooperare pe plan local și regional, între operatorii de infrastructuri și servicii critice, publici sau privați și furnizorii de servicii și echipamente specializate, pentru realizarea planurilor de reziliență elaborate în acest sens.**

Directiva CE – 114/2008, din 08 Decembrie 2008

7). Analiza modului de elaborare și aplicare a obligațiilor ce revin operatorilor de infrastructuri critice, precizate de legislația națională și Directiva Europeană CE – 114, din 08 Decembrie 2008

In condițiile Directivei 114-2008, la toate Infrastructurile Critice, vor exista:

a). Ofițer de Legătură pentru Securitatea Infrastructurilor Critice sau un echivalent al acestuia, pentru a facilita cooperarea și comunicarea cu autoritățile naționale competente în materie de protecție a infrastructurilor critice.

b). Planuri de Securitate pentru Operatori (PSO) sau măsuri echivalente, care să conțină o identificare a elementelor importante, o evaluare a riscurilor și identificarea, selectarea și stabilirea priorităților în ceea ce privește contramăsurile și procedurile.

Statele membre ale Uniunii Europene, sunt obligate să pună în aplicare măsurile necesare pentru a se conforma prezentei directive până la 12 ianuarie 2011, informând Comisia Europeană în această privință, comunicând totodată și textele cuprinzând măsurile elaborate, data publicării lor oficiale precum și tabelele de concordanță stabilite de această directivă.

23.12.2008

RO

Jurnalul Oficial al Uniunii Europene

L 345/75

DIRECTIVA 2008/114/CE A CONSILIULUI

din 8 decembrie 2008

privind identificarea și desemnarea infrastructurilor critice europene și evaluarea necesității de îmbunătățire a protecției acestora

(Text cu relevanță pentru SEE)

11

Planul de Securitate pentru Operatori (PSO)

Planurile de securitate pentru operatori (PSO), vor respecta următoarele cerințe de bază:

1). Identificarea elementelor critice;

2). Efectuarea unei analize de risc bazate pe scenarii de amenințări majore, pe punctele vulnerabile ale fiecărui element și pe impactul potențial;

3). Identificarea, selectarea și stabilirea priorităților în ceea ce privește contramăsurile și procedurile, făcându-se distincție între:

a) măsurile permanente de securitate, care identifică investițiile de securitate indispensabile și mijloacele care sunt relevante pentru utilizarea în orice situație, cum ar fi:

- măsurile tehnice (inclusiv instalarea de mijloace de detectare, de control al accesului, de protecție și de prevenire);
- măsuri organizatorice (inclusiv proceduri pentru gestionarea alertelor și a crizelor);
- măsuri de control și verificare;
- comunicare și informarea populației;
- formarea personalului specializat pentru intervenție;
- securitatea sistemelor de informații;

b) măsuri de securitate graduale, care pot fi activate în funcție de diferitele niveluri ale riscurilor și amenințărilor.

Contribuția partenerilor publici și privați, pentru protecția infrastructurilor critice

Concluzii, privind contribuția partenerilor publici și privați, pentru protecția infrastructurilor și serviciilor critice care asigură, în cadrul comunităților locale, securitatea și siguranța cetățenilor

Concluziile rezultate la finalizarea activităților enumerate anterior, vor fi utilizate pentru elaborarea unui **model de "proces decizional"**, care să permită abordarea, discutarea și soluționarea subiectelor relevante pentru securitatea și siguranța cetățenilor și a comunităților, precum și luarea de decizii optime, având drept scop reducerea vulnerabilităților și creșterea **"capacității de reziliență"** a serviciilor și infrastructurilor critice vitale cetățeanului și comunităților sau la nivel regional și național.

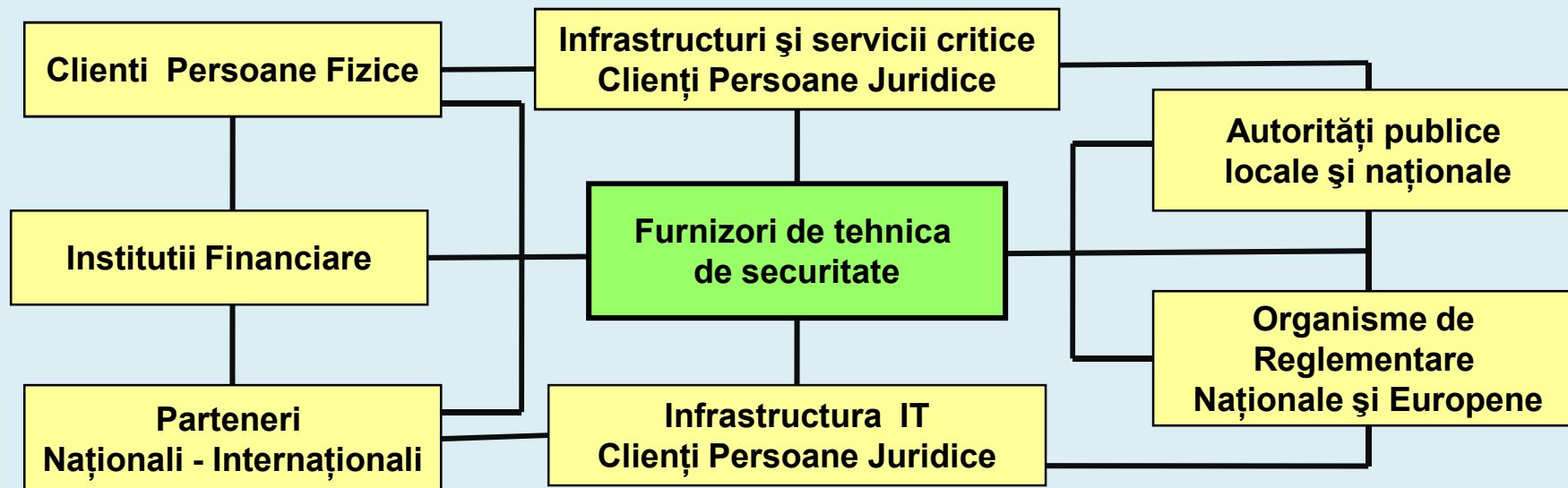
„Procesul decizional model” va fi aplicat pentru evenimente și scenarii diverse, inclusiv cele bazate pe experiențe anterioare, selectându-se cele care au probabilitate ridicată de a se repeta în viitor, având ca scop elaborarea unor soluții de îmbunătățire a protecției infrastructurilor critice care asigură siguranța și securitatea individului și a comunităților locale.

Soluțiile aprobate vor fi puse în practică de către operatorii de infrastructuri și servicii critice, cu ajutorul autorităților locale și a partenerilor din sectorul public și privat.

Contribuția partenerilor publici și privați, pentru protecția infrastructurilor critice

O contribuție și responsabilitate importantă, pentru protecția infrastructurilor și serviciilor critice, revine companiilor private care activează în sectorul de securitate, membre ale Asociației Române pentru Tehnica de Securitate.

Aportul acestora, prin specialiști, propuneri de soluții tehnice inteligente și utilizarea de echipament specializat, conform domeniului de activitate și competențelor fiecăreia, este deosebit de important în elaborarea și realizarea soluțiilor și ulterior instruirea personalului dedicat, exploatarea, întreținerea și perfecționarea sistemelor de monitorizare și protecție în caz de dezastre, fenomene și procese tehnologice cu potențial de risc ridicat, specifice fiecărui proiect de reziliență dezvoltat pentru infrastructurile și serviciile critice care funcționează pe plan local sau regional.



Specialiștii din cadrul companiilor membre ale Asociației Române pentru Tehnica de Securitate, pot și este necesar să contribuie activ la promovarea și susținerea inițiativelor de elaborare a unor principii și proceduri de lucru specifice protecției și rezilienței infrastructurilor și serviciilor critice, perfecționarea protecției și siguranței cetățeanului precum și propuneri de îmbunătățire a unor normative comunitare sau a legislației naționale în domeniu, luând în considerare prevederile Directivelor și normativelor europene în vigoare.

De referință în acest domeniu este în prezent Directiva CE – 114/2008, din 08 Decembrie 2008, care constituie un prim pas în direcția identificării și a desemnării Infrastructurilor Critice Europene (ICE) și a evaluării necesității de îmbunătățire a protecției acestora în toate statele membre ale Uniunii Europene.

In prezent, este în curs de elaborare Directiva europeană, care va reglementa protecția și măsurile minime de reziliență, ***pentru domeniul informațiilor infrastructurilor și serviciilor critice și tehnologia informațiilor***, urmând ca ulterior să fie elaborate, supuse dezbaterii și aprobate Directivele și normative specifice pentru toate sectoarele și serviciile considerate critice de către programul european de protecție a infrastructurilor critice (EPCIP).

**Directiva 2008/114/CE a Consiliului din 8 Decembrie 2008
Termeni de referinta**

“DIRECTIVA 2008/114/CE a Consiliului Europei, privind identificarea și desemnarea infrastructurilor critice europene și evaluarea necesității de îmbunătățire a protecției acestora”, obligă prin prisma legislației europene ca, în statele membre ale UE (implicit ROMANIA), protecția și reziliența infrastructurile critice să devină o prioritate națională, având o contribuție deosebită la securitatea și stabilitatea fiecărei națiuni și prin acest aspect un factor de securitate, încredere și bună colaborare între statele europene.

Participarea specialiștilor din sectorul public și cel privat la elaborarea măsurilor de Protecție și Reziliență a Infrastructurilor și Serviciilor Critice

Importanța participării specialiștilor, din sectorul public și cel privat, la elaborarea măsurilor de Protecție a Infrastructurilor și Serviciilor Critice, vitale individului și funcționării societăților moderne, trebuie înțeleasă prin necesitatea de a asigura cunoașterea, de către toți factorii implicați, a sarcinilor și atribuțiilor ce le revin, pentru prevenirea, pe timpul și după rezolvarea unor situații de urgență, generate de vulnerabilități sau elemente de risc diverse.

Prin efort comun este posibil să fie creat un cadru unitar și coerent de acțiune pentru prevenirea și gestionarea unor situații de urgență diverse, reducerea de pierderi economice semnificative, vătămarea personalului propriu și a populației precum și asigurarea unui răspuns optim, adecvat fiecărui tip de risc identificat.

Vă mulțumim pentru atenție !



**FUNDATIA EURISC
INSTITUTUL EUROPEAN PENTRU MANAGEMENTUL RISCULUI,
SECURITATII SI COMUNICARII**

C.P. 2-111, Bucuresti, Romania

Tf. 021 212 2102 Tf. / Fax : 021 319 3279

E-mail: eurisc@eurisc.org

www.eurisc.org