

**SESAM** Försvarssektorns Användargrupp för Software Engineering

**SNSS** Svenskt Nätverk för Systemsäkerhet

i samarbete med  
**FMV** och **KTHs** centrum för Inbyggda system  
inbjuder till seminariet



**System Safety**  
**in**  
**Software-Intensive**  
**Systems**

Dr. Nancy Leveson  
Professor at the Massachusetts Institute of Technology, MIT

**21-22 maj 2008**

KTH, Stockholm

Software allows unprecedented levels of complexity and new failure modes that are starting to overwhelm the standard approaches to ensuring safety. The causes of accidents are even changing. This seminar will focus on the unique problems involved in building software-controlled systems. Emphasis will be on procedures and techniques that are practical enough to be applied to projects today. Real-project experiences with these techniques in different application areas will be described and recent software-related accidents will be reviewed and analyzed.

The first day of the seminar will include a novel model of accident causation, STAMP, and the new approach to hazard analysis built upon it, STPA. These techniques have the ability to handle social and organizational factors as well as technical aspects in accidents and incidents, making them better suited to address the increasing complexity of the systems currently being developed, than the traditional safety analysis methods. The second day will focus on some of the requirements, design and human factor issues covered by the book 'Safeware: System Safety and Computers'. For those not able to attend both days and with interest mainly in the latest hazard analysis techniques, the first day of the seminar will be the recommended choice.

---

## PROGRAM (preliminary)

### Wednesday May 21

- 08.30-09.30 Registration and coffee
- 09.30-10.00 Introduction (*of SESAM, SNSS, ICEs\* and the author*)
- 10.00-12.10 The problem and overall approach (*Nancy Leveson*)
- 12.15-13.15 Lunch
- 13.15-15.00 STAMP and hazard analysis (*Nancy Leveson*)
- 15.00-15.30 Coffee break
- 15.30-17.30 STAMP and hazard analysis (cont'd)
- 18.00-21.00 Buffet and informal discussions

### Thursday May 22

- 09.00-10.00 Requirements (*Nancy Leveson*)
- 10.00-10.30 Coffee break
- 10.30-12.15 Design (*Nancy Leveson*)
- 12.15-13.15 Lunch
- 13.15-14.30 Design (cont'd)
- 14.30-15.00 Coffee break
- 15.00-17.00 Human-computer interaction (*Nancy Leveson*)

**Programansvarig:** Inga-Lill Bratteby-Ribbing  
Strategisk specialist Programvarusäkerhet  
FMV AK Gem  
inga-lill.bratteby-ribbing@fmv.se

**Upplysningar:** Anna Kåsjö, 08-510 51866 eller 070-716 9702

**Plats:** KTH, Lindstedtsv 22, Sal F1 (entreplan), Stockholm

**Avgift:** SESAM är en icke vinstdrivande, ideell förening. De deltagaravgifter, som tas ut är därför beräknade till självkostnadspris.

**21-22 maj, 1500:-** (Inkl förtäring)

Programmet omfattar 2 dagar, men för den som enbart kan avsätta en dag ges möjlighet till lägre avgift enligt nedan:

**21 maj, 1000:-** (Inkl förtäring)     **22 maj, 800:-** (Inkl förtäring)

Student, mot uppvisande av studentleg, betalar endast 100 kr per dag, kaffe och lunch ingår men ej buffén.

**21 maj, 100:-**       **22 maj, 100:-**

**Anmälan:** Sista anmälningdag **29 april** 2008  
Anmälan är bindande  
Avgiften faktureras

**Anmälan skickas till:**

SESAM-sekretariatet  
Kåsjös Kontor  
Odengatan 28, 4 tr  
113 51 STOCKHOLM

Tel: 08-510 518 66, 070-716 9702  
Fax: 08-380 789  
E-post: anna@kasjoskontor.se

---

## Anmälan

till seminariet den 21-22 maj 2008 på KTH

Namn: \_\_\_\_\_

Org/Företag: \_\_\_\_\_

Postadress: \_\_\_\_\_

\_\_\_\_\_

Telefon: \_\_\_\_\_ Fax: \_\_\_\_\_

E-post: \_\_\_\_\_

Faktureringsadress om annan än ovan:

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

**Dr. Nancy Leveson** is a Professor in the Aeronautics and Astronautics Dept. at the Massachusetts Institute of Technology (MIT). Previously she was Boeing Professor of Computer Science and Engineering at the University of Washington. She has served as Editor-in-Chief of IEEE Trans. on Software Engineering. She received the ACM 1999 Allen Newell Award for "establishing the foundations of software safety" and the 1995 AIAA Information Systems Award for "developing the field of software safety and for promoting responsible software and system engineering practices where life and property are at stake."

Dr. Leveson consults widely on safety-critical systems for both government and industry and has worked with aerospace, nuclear power, transportation, aircraft, and medical systems.

Dr. Leveson is a member of the National Academy of Engineering (NAE) and author of a book, "Safeware: System Safety and Computers". A draft of her next book, 'A New Approach To System Safety Engineering' is available on the web site <http://sunnyday.mit.edu>.

---

**SESAM**, Försvarssektorns Användargrupp för Software Engineering, är ett sedan 1988 fungerande samverkansnätverk för projektövergripande och företagsneutral kunskapsuppbyggnad och kunskapsspridning inom området programvaruintensiva försvarssystem.

SESAM bedriver sin verksamhet på olika sätt bl a genom:

- Arbets- eller intressegrupper med deltagande av flera medlemsintressenter. ett exempel är IG Programvarusäkerhet, kontaktperson Inga-Lill Bratteby-Ribbing, FMV.
- Större eller mindre utrednings/utvärderingsprojekt
- Redovisningar av årets projekt som sker i samband med höstseminariet
- Teknikspaning med efterföljande informationsspridning till medlemmarna
- Seminarier med interna och externa föreläsare kring aktuella frågor för SESAM
- Informationsspridning bl a genom SESAM hemsida, CD till medlemmarna

Intressent i SESAM kan vara försvarsmyndighet och företag eller institution som har utvecklingsuppdrag/beställning från försvarsmyndighet. Av intressent krävs viss garanterad arbetsinsats i arbetsgrupperna.

SESAM styrs av ett råd, som är sammansatt av repr för intressenterna. Ordf är f.n. Claes Wadsten, Saab Aerotech, och vice ordf Curt Merckell, Saab Bofors Dynamics.

Läs mer om SESAM på <http://sesam.smart-lab.se>

**SNSS**, Svenskt Nätverk för Systemsäkerhet, är en ideell förening som bildades 1997. Föreningen syfte är att sprida och öka kunskapen om, och intresset för, systemsäkerhet.

Med systemsäkerhet avses egenskapen hos ett system att inte orsaka skada på person, egendom eller yttre miljö.

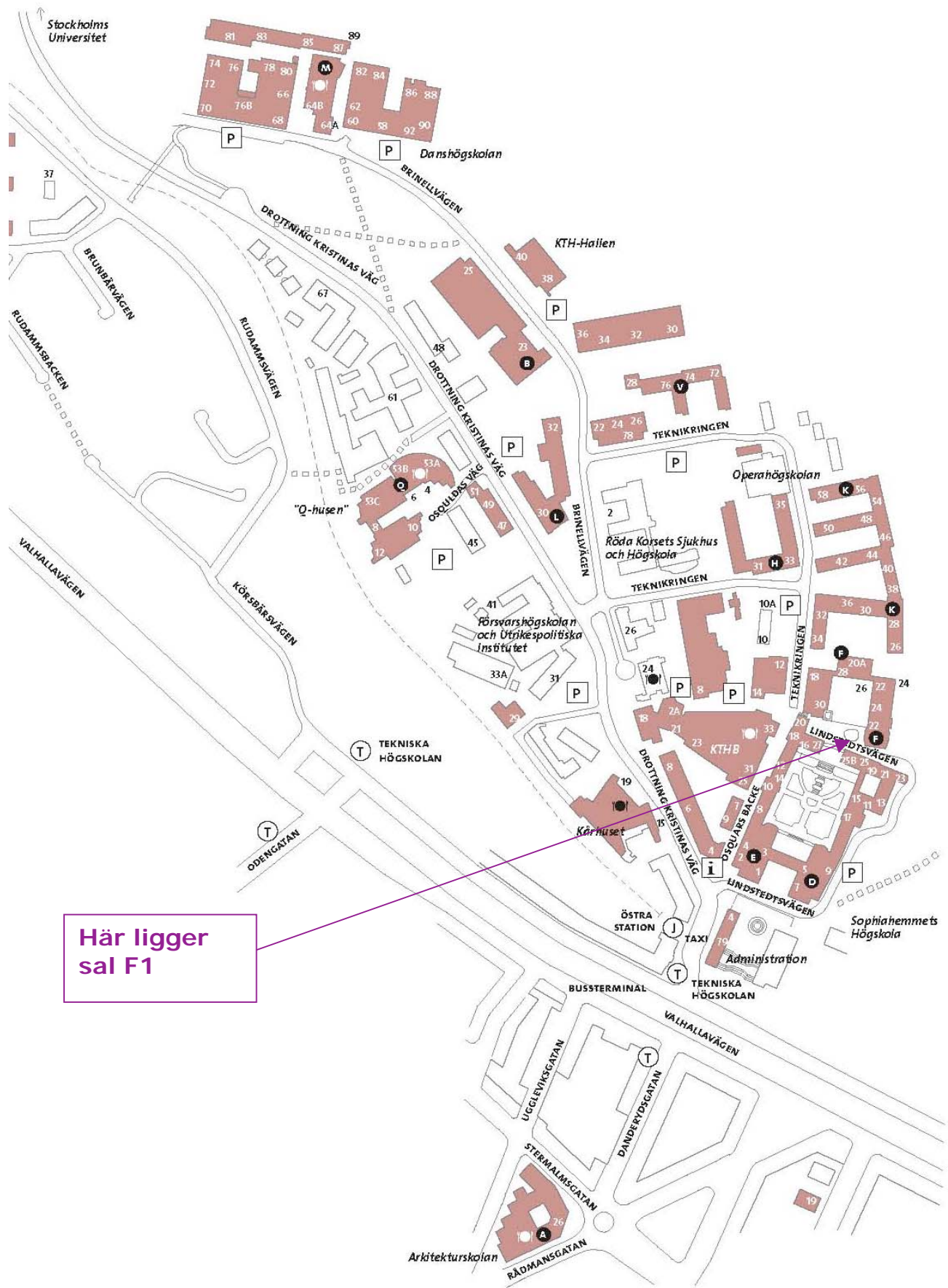
SNSS syfte är att etablera och sprida Systemsäkerhetskompetens och bidra till säkrare system och produkter.

SNSS arbetar med att:

- arrangera möten med föredrag
- arrangera studiebesök
- arrangera seminarier
- utgöra ett forum för erfarenhets- och informationsutbyte

Området systemsäkerhet är tvärvetenskapligt vilket återspeglas bland våra medlemmar som representerar verksamhetsområden som energi-, transport-, försvars- och medicin-teknik. Det betyder också att SNSS medlemmar har olika typer av kompetens som ingenjörer, beteendevetare, jurister och forskare.

Läs mer om SNSS, föreningens stadgar samt systemsäkerhet på [www.snss.nu](http://www.snss.nu)



Här ligger  
sal F1