

A COMMUNITY CLUB ON SAFETY-CRITICAL SYSTEMS

Felix Redmill
London, UK

ACS Workshop
Adelaide, October 2002

BACKGROUND 1980s

- Software-based systems used for most control functions
- Is software mature enough for this?
- If we can't prove software correct, can we prove it safe?
- Can we control software adequately?
- How can we make software safe?

But

- Market forces dictated the use of software
- Software-based systems can improve safety

So:

- What to do to gain confidence that a system is safe enough

FR

2

SAFETY-CRITICAL SYSTEMS CLUB OBJECTIVES

- Raise awareness of safety issues
 - That systems are safety-critical
 - That steps need to be taken to achieve adequate safety
 - Safety engineering
- Facilitate technology transfer
- Focus on current and emerging practices in safety engineering, software engineering, and standards that relate to safety in processes and products

FR

3

SUGGESTED ADVANTAGES

- Increase the rate of dissemination of useful technologies
- Prevent the spread of flawed technologies by the rapid communication of experience
- Improve the industrial testing of new technologies
- Bring industrialists together to plan feedback to academia and to co-ordinate the sponsorship of research
- Improve the choice and application of technology
- Accelerate the feedback to academia of experience in the use of technologies
- Improve safety-critical systems that are supplied to industry
- Facilitate the targeting of research
- Accelerate the improvement of flawed but useful technologies

FR

4

ORGANISATION

- Secretariat (Joan Atkinson, University of Newcastle upon Tyne)
 - Membership
 - Event venues and registration
 - All money
 - Mailshots
- Co-ordinator (FR, London)
 - Plan events
 - » Programmes, speakers, publicity
 - Annual Symposium
 - » Programme, authors, papers, editing, publisher, tutorial, sponsorship
 - Plan and edit newsletter
 - » Authors

FR

5

INDEPENDENCE

- Non-profit organisation
- Co-operates with all bodies but independent
- Sponsorship buys publicity but not allegiance
- Results
 - Club atmosphere
 - Speakers say what they wouldn't elsewhere
 - Delegates initiate discussion that they wouldn't elsewhere

FR

6

INCOME

- Initial subsidy by DTI
- Membership subscriptions
- Seminar and tutorial charges
- Annual symposium
 - Two days of paper sessions
 - One-day tutorial
 - Tools fair charges
 - Sponsorship
- Members' reduction in event fee = annual subscription

FR

7

SUMMARY OF THE CLUB'S EVENTS May 1991 - May 2002

<i>Type of event</i>	<i>No. of events</i>	<i>No. of speakers</i>	<i>No. of delegates</i>	<i>Average No. of delegates per event</i>
Seminars	40	266	3386	85
Symposia	10	161	1515	152
Tutorials	21	28	1252	60
TOTALS	71	455	6153	87

FR

8

PUBLICATION OF PAPERS AND ARTICLES May 1991 - May 2002

<i>Type of publication</i>	<i>Number of publications</i>	<i>No. of papers or articles published</i>
Books	11	188 papers
Newsletter	33 issues	197 articles

FR

9

LIMITS TO SUCCESS

- Low academic participation
- Inability to get to SMEs (small & medium-sized enterprises)
- Attracting engineers, project managers, risk analysts, etc., but not senior managers and strategists

FR

10

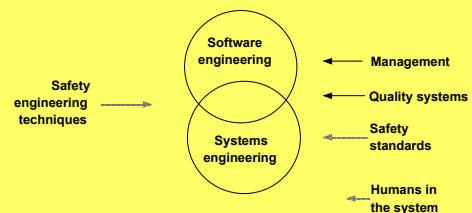
CHANGES IN THE DOMAIN SINCE 1991

- Awareness
- Safety engineering techniques
- Standards on safety
- Safety assessment
- The safety case
- Competence
- Human factors
- Safety-related information systems
- COTS
- Safety management and culture

FR

11

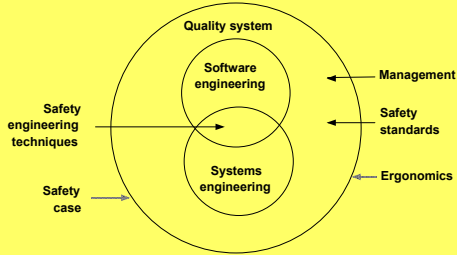
PERCEPTION WITHIN THE FIELD IN 1991



FR

12

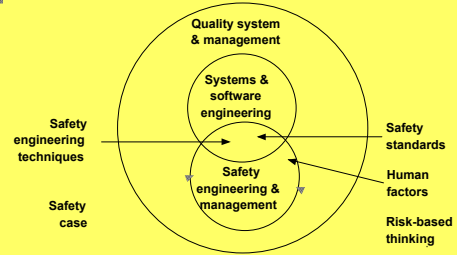
PERCEPTION WITHIN THE FIELD IN 1996



FR

13

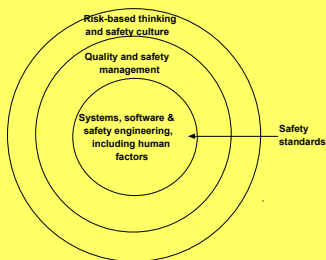
PERCEPTION WITHIN THE FIELD IN 2002



FR

14

POSSIBLE TREND IN THE FIELD



FR

15

TECHNICAL SCOPE FOR CLUB ACTIVITIES

1

- Awareness
 - Our systems are safety-critical
 - We are expected to carry out risk analyses
 - Legal issues
 - Accidents and their causes
- Safety engineering techniques
 - Risk-based thinking
 - Hazard identification
 - Hazard analysis
 - Non-engineering perspectives (e.g. social science)
- Standards on safety
 - IEC 61508 and others
 - Interpretations
 - Feedback on experiences

FR

16

TECHNICAL SCOPE FOR CLUB ACTIVITIES

2

- Safety assessment
 - Scope and content
 - Legal and regulatory requirements
 - Advantages and reasons
 - Credentials of practitioners
- The safety case
 - Understanding
 - Methods of development
 - Tools
 - Experience - difficulties and lessons
- Competence
 - Employment, training, deployment, monitoring
 - Regulations, legal requirements, if any
 - Evolution towards responsible practice

FR

17

TECHNICAL SCOPE FOR CLUB ACTIVITIES

3

- Human factors
 - Holistic system view
 - Psychology of human error
 - Human reliability assessment
 - Incorporation of human factors in risk analysis
- Risk analysis
 - Techniques
 - Integration of human reliability assessment
 - Risk-based thinking as a culture
- Safety-related information systems
 - The need to extend risk-based thinking

FR

18

TECHNICAL SCOPE FOR CLUB ACTIVITIES

4

- **COTS**
 - The debate
 - Recent research in justifying COTS
- **Safety management and culture**
 - Limitations of management systems
 - Nature of culture and its development
- **And more ...**

FR

19

CONCLUSIONS

- **The UK Safety-Critical Systems Club is in its 12th year**
- **Objectives to raise safety awareness and transfer technology**
- **It has conducted a number of activities**
- **Its experiences could be useful to another club**
- **Perception of the safety-critical systems field by its practitioners has developed and is developing**
- **There are many areas that require awareness-raising and technology transfer**

FR

20