ADELARD

Security risk assessment: between snake oil and science

Robin E Bloomfield
Robert J Stroud
25 Jan 2014

pt220v01d

Exmouth House 3–11 Pine Street London EC1R 0JH
T +44 20 7832 5850 F +44 20 7832 5853 E office@adelard.com W www.adelard.com

Overview

- Introductions
- Context and challenge
- Overall approach
  - Some elements
- Discussion and conclusions

Background

- Practitioner and researcher
  - Adelard LLP
  - CSR City University London
- Adelard
  - Specialised consultancy, PhD entry level
  - Policy to technical
  - Large infrastructure to components
  - Advice and assessment, even if unwelcome
  - Working on security and safety
    - Transport systems
    - Awareness course for safety engineers and managers

Security risk assessment: between snake oil and science?

- If we are to shape decisions about critical infrastructure we need to make comparative judgements of risk and uncertainty. We need to assess the risks from technology that has not yet been implemented, of systems that don't yet exist, operated by turbulent organisations in a threat environment that is unknown or unknowable.
- Particularly interested in large scale systems with societal risks
  - Methodology development
  - Risk assessment
  - Research informed practice and vice versa

Conclusion

- Risk assessment/prediction provides many useful outputs
  - an estimate of the risk is .. ~~not~~/only one... of them

Safety and security

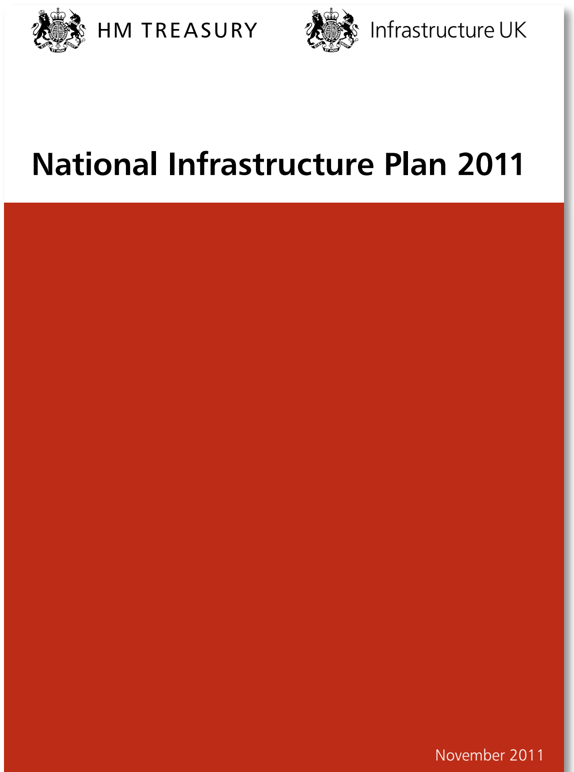
- Safety – concerns the damage the system can do to the environment
- Security – the damage the environment (in a broad sense) does to the system

If it's not secure, it's not safe

Context - risk assessment and policy

- EEIG UK Infrastructure Plan
- UK National Risk Assessment
- Risks within ERTMS specification and deployment
- Research into security informed safety (Sesamo)

National Infrastructure Plan


HM TREASURY Infrastructure UK

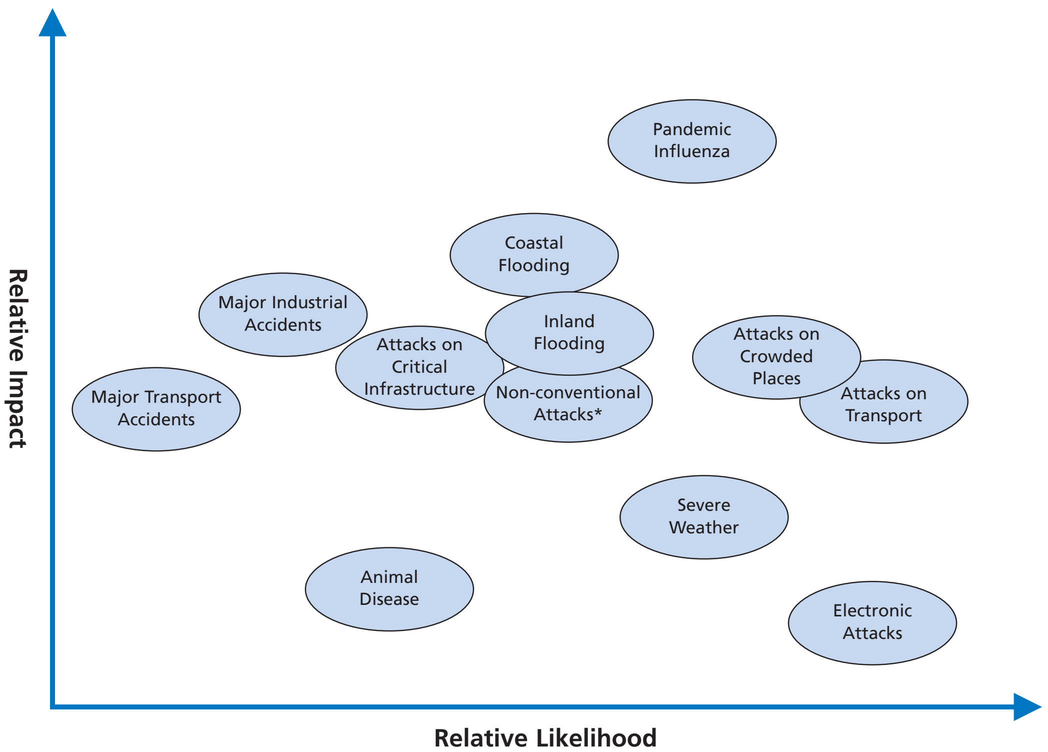
National Infrastructure Plan 2011

November 2011

Chapter 1	Introduction: the UK's infrastructure performance	13
Chapter 2	Priority programmes and projects	19
Chapter 3	Sectoral infrastructure plans	31
	The UK's transport systems	31
	The UK's energy systems	52
	The UK's communications systems	65
	The UK's environmental systems	72
	Intellectual capital	84
	Infrastructure investment in Scotland, Wales and Northern Ireland	85
Chapter 4	Addressing opportunities and risks across sectors	89
Chapter 5	Financing and funding the planned investment	97
Chapter 6	Securing efficient delivery of infrastructure	107
Chapter 7	Next steps	119
Annex A	Progress against National Infrastructure Plan 2010	127
Annex B	Infrastructure investment pipeline data	131
Annex C	Priority programmes and projects: milestones	133
Annex D	Infrastructure performance and cost: methods, sources and data	141

UK National Risk Register

Figure 1: ***An illustration of the high consequence risks facing the United Kingdom***

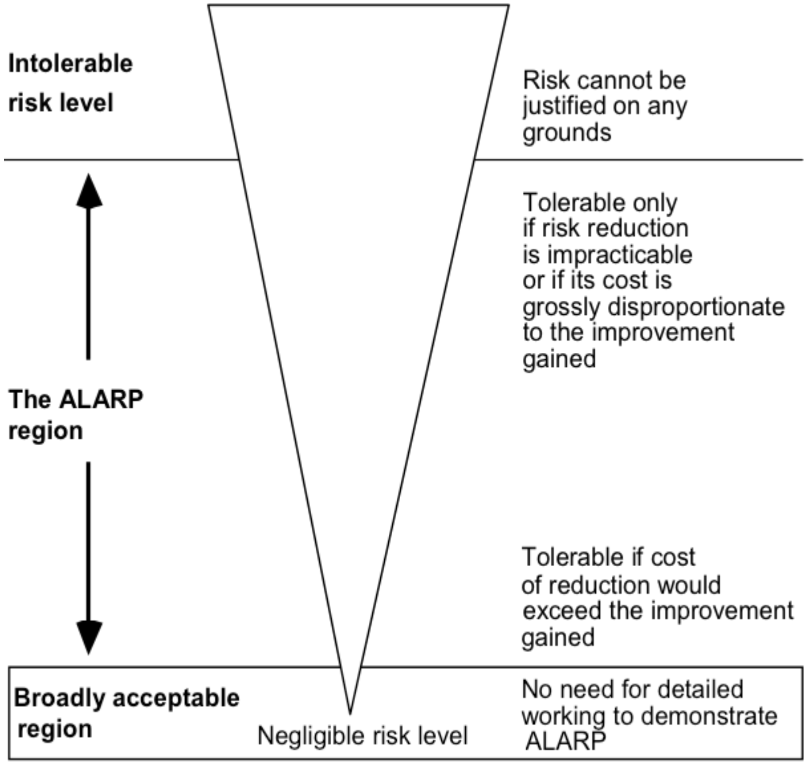


* The use of some chemical, biological, radiological and nuclear (CBRN) materials has the potential to have very serious and widespread consequences. An example would be the use of a nuclear device. There is no historical precedent for this type of terrorist attack which is excluded from the non-conventional grouping on the diagram.

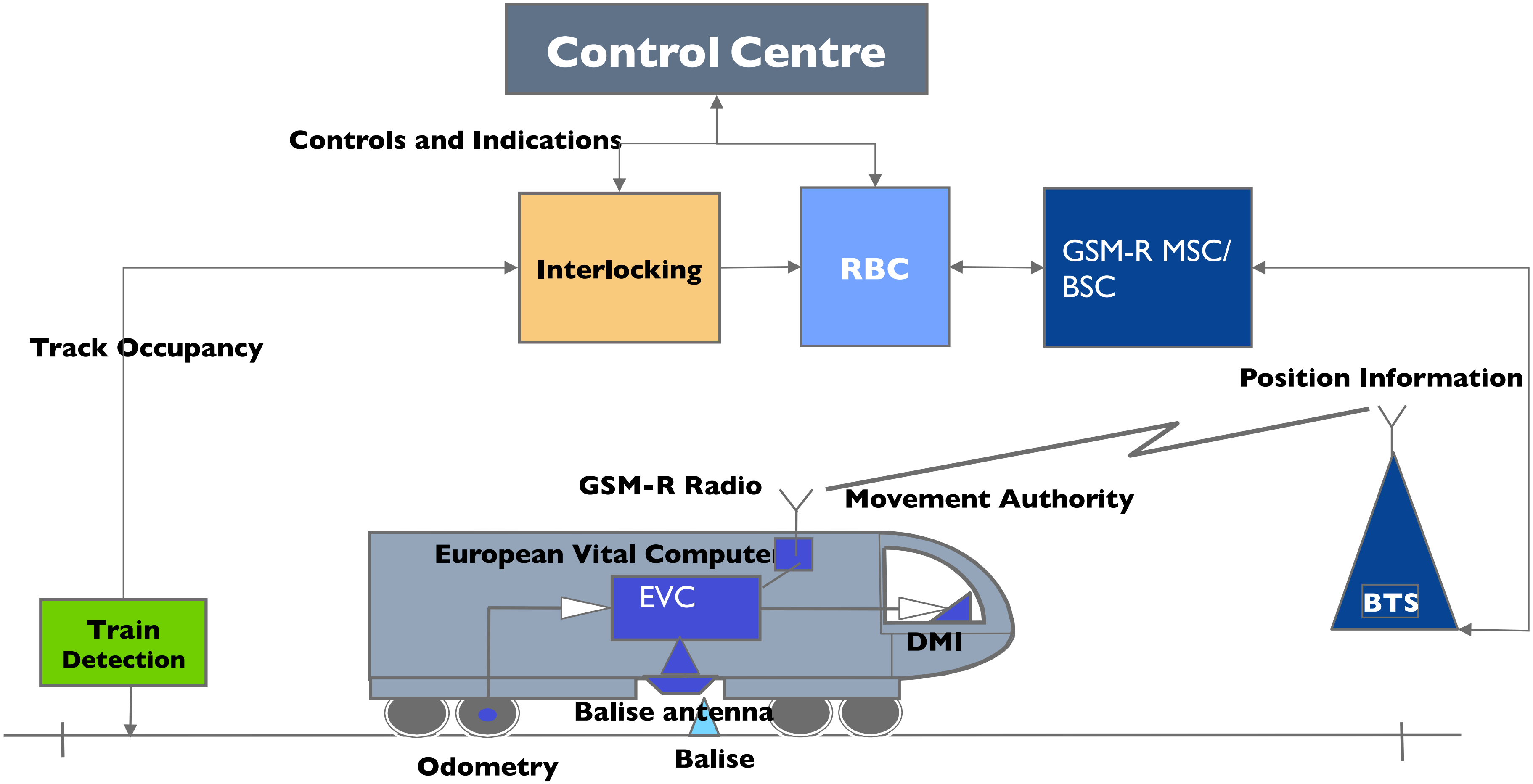
National Risk Register

- National Risk Register illustrates the kinds of contingency which primarily drive planning
  - by government and the emergency services and for which organisations, individuals, families and communities
  - the selection excludes some risks that are classified for reasons of national security
- Risks are relative – they aim to compare the likelihood and impact of events with each other;
  - only look at risks of emergencies in the UK
- Risks to the country as a whole, and so do not take into account local conditions which may be different to the national picture;
- Focus is major emergencies under the Civil Contingencies Act.

“Carrot” diagram



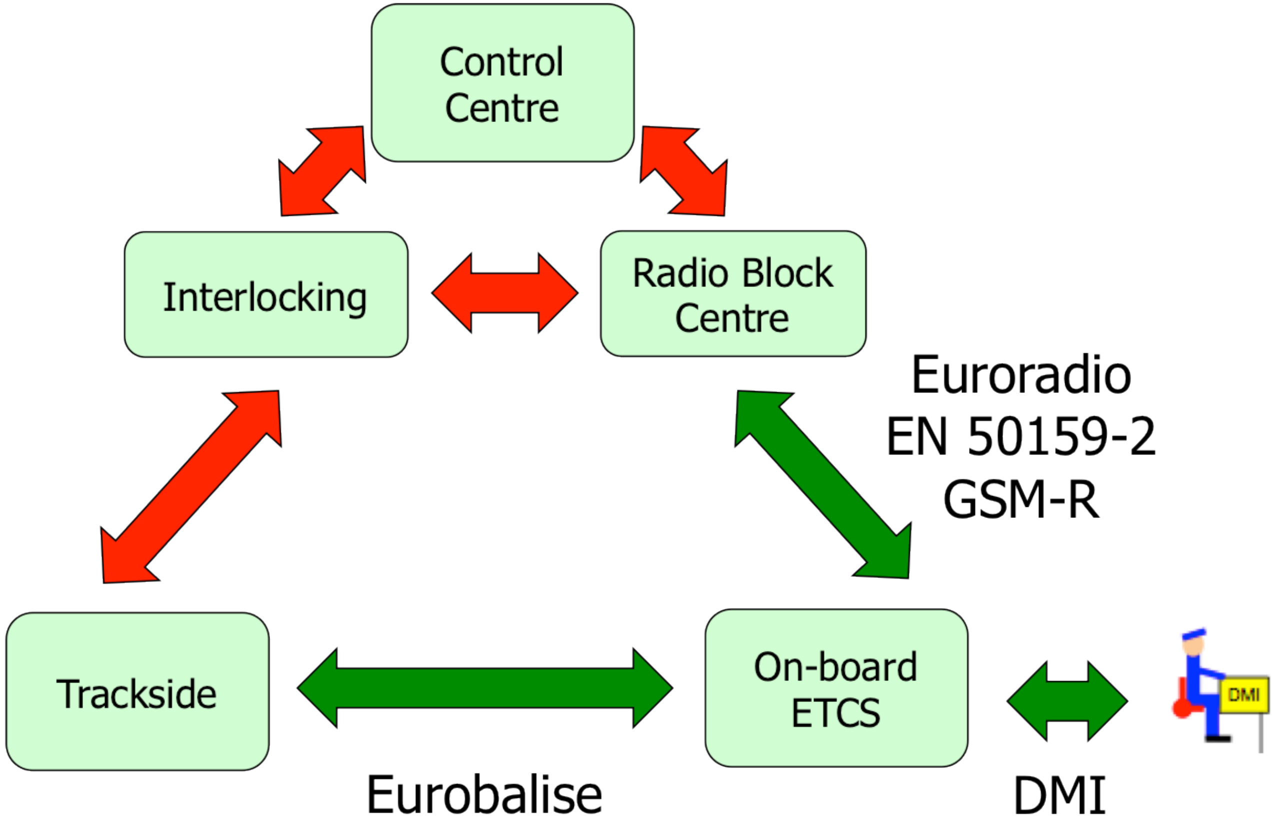
ERTMS SYSTEM ARCHITECTURE



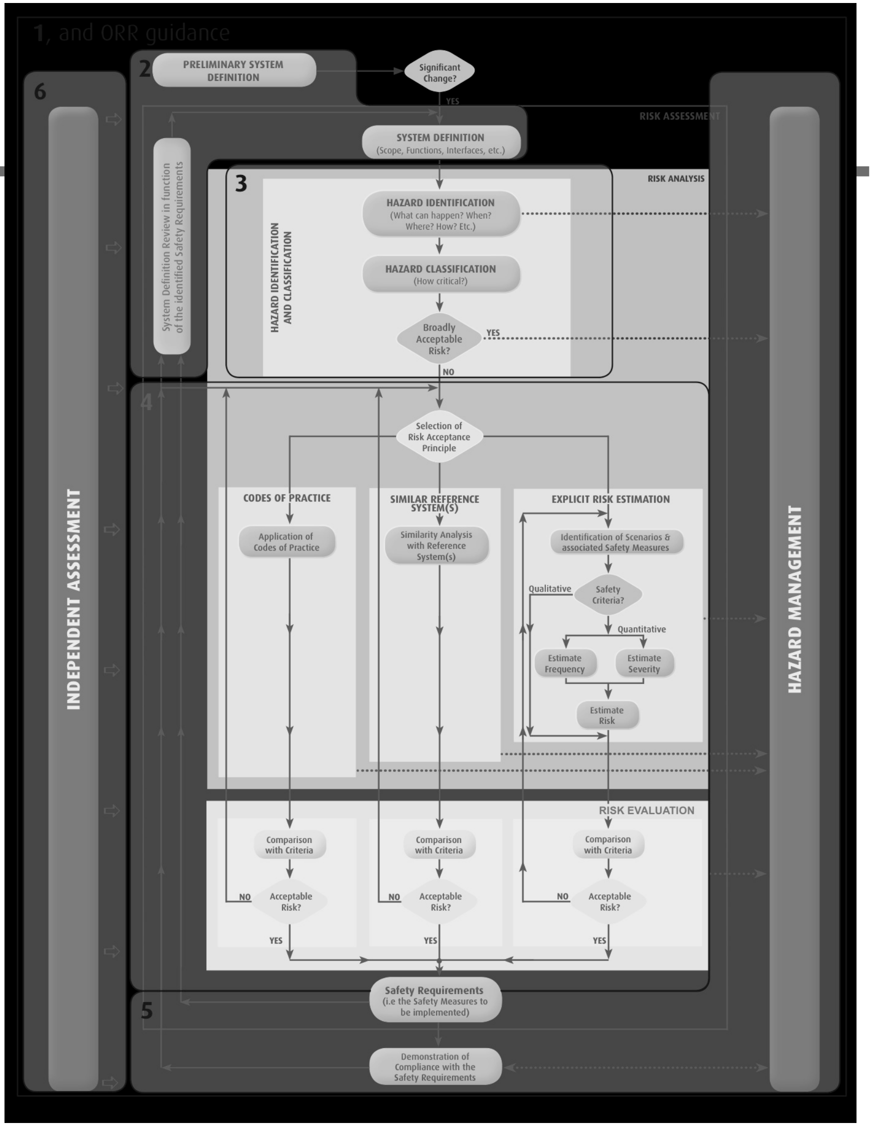

STOP
HS2

ERTMS AND LEGACY SYSTEMS

ERTMS CONCEPTUAL ARCHITECTURE



Common Safety Method

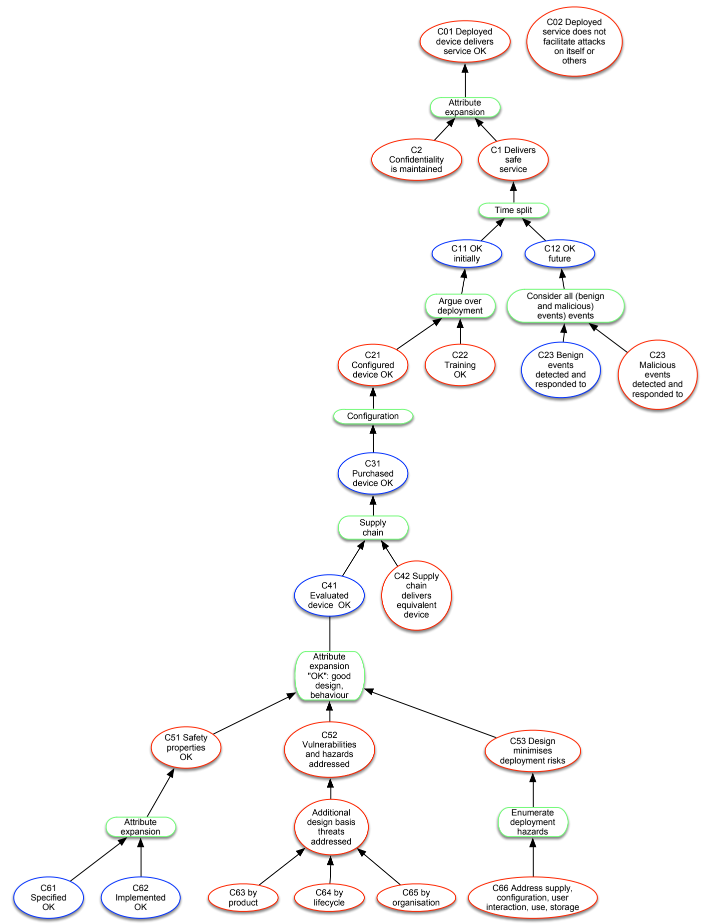


Common Safety Method (CSM) For Railways

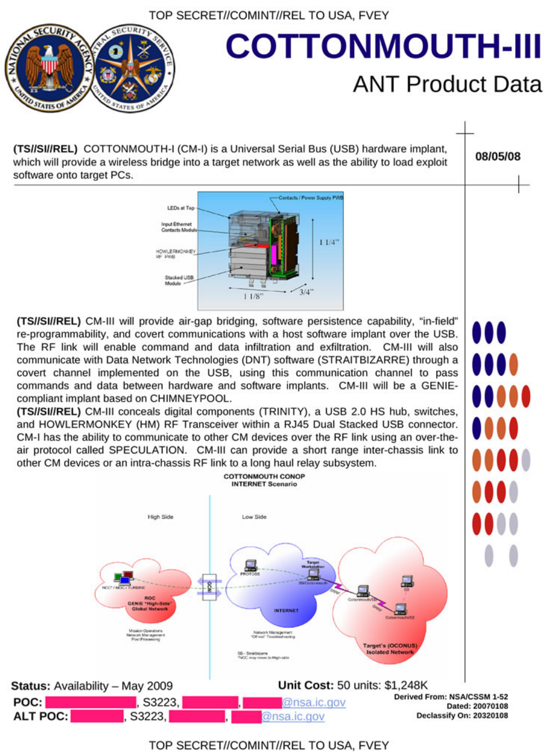
- EC Regulation 352/2009 sets out a Common Safety Method on risk assessment and evaluation for the mainline railway
- The CSM describes a risk management framework that uses using one or more of the following risk acceptance principles:
  - application of codes of practice
  - comparison with similar systems (reference systems)
  - explicit risk estimation
- The process is iterative and ends when the proposer is satisfied that for each hazard there is compliance with the safety requirements and measures identified, and that overall the risk is controlled as far as is reasonably practicable

Initial analysis of impact of security

- What impact does security have on the safety case?
- Some observations:
  - Supply chain integrity
  - Malicious events post deployment
  - Design changes to address user interactions, training, configuration, vulnerabilities
  - Additional functional requirements - security controls
  - Possible exploitation of the device/service to attack itself or others
- Evidence of effectiveness of controls hard to find



World of Mandiant, Snowden



TOP SECRET//COMINT//REL TO USA, FVEY

COTTONMOUTH-III

ANT Product Data

08/05/08

(TS//SI//REL) COTTONMOUTH-I (CM-I) is a Universal Serial Bus (USB) hardware implant, which will provide a wireless bridge into a target network as well as the ability to load exploit software onto target PCs.

(TS//SI//REL) CM-III will provide air-gap bridging, software persistence capability, "in-field" re-programmability, and covert communications with a host software implant over the USB. The RF link will enable command and data infiltration and exfiltration. CM-III will also communicate with Data Network Technologies (DNT) software (STRAITBIZARRE) through a covert channel implemented on the USB, using this communication channel to pass commands and data between hardware and software implants. CM-III will be a GENIE-compliant implant based on CHIMNEYPOOL.

(TS//SI//REL) CM-III conceals digital components (TRINITY), a USB 2.0 HS hub, switches, and HOWLERMONKEY (HM) RF Transceiver within a RJ45 Dual Stacked USB connector. CM-I has the ability to communicate to other CM devices over the RF link using an over-the-air protocol called SPECULATION. CM-III can provide a short range inter-chassis link to other CM devices or an intra-chassis RF link to a long haul relay subsystem.

COTTONMOUTH CONOP
INTERNET Scenario

Status: Availability – May 2009

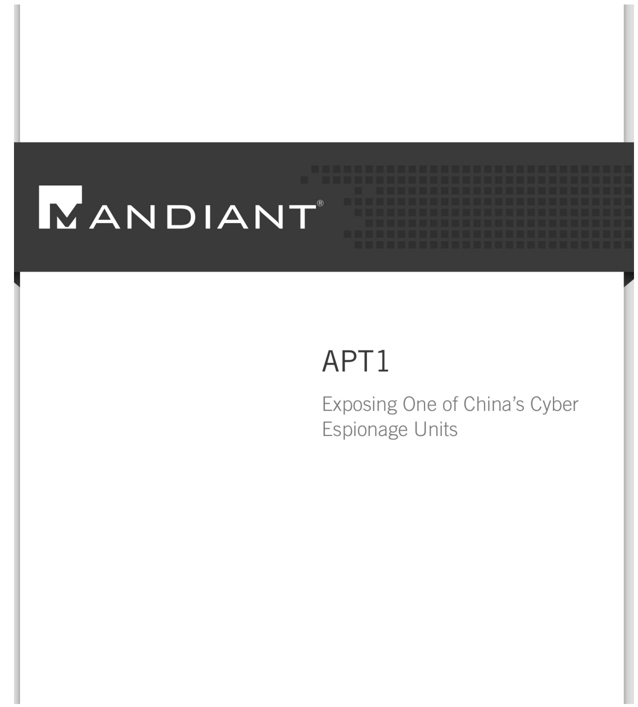
Unit Cost: 50 units: $1,248K

POC: [redacted], S3223, [redacted], [redacted]@nsa.ic.gov

ALT POC: [redacted], S3223, [redacted], [redacted]@nsa.ic.gov

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

TOP SECRET//COMINT//REL TO USA, FVEY



http://leaksource.wordpress.com/2013/12/30/nsas-ant-division-catalog-of-exploits-for-nearly-every-major-software-hardware-firmware/

http://intelreport.mandiant.com/

And …

```
  BOOL result; // eax@4

  if ( fdwReason && fdwReason == 1 && (DisableThreadLibraryCalls(hinstDLL),
sub_10001186()) )
    result = sub_1000123A(hinstDLL);
  else
    result = 0;
  return result;
}

//----- (10001030) --------------------------------------------------------
int __stdcall StartAddress(LPCWSTR lpString2)
{
  int v1; // eax@2
  UINT v2; // edi@5
  int v4; // [sp-4h] [bp-414h]@4
  int v5; // [sp+0h] [bp-410h]@4
  WCHAR FileName; // [sp+208h] [bp-208h]@4

  if ( lpString2 )
  {
    v1 = lstrlenW(lpString2) + 1;
    if ( v1 > 260 )
      v1 = 260;
    lstrcpynW(&FileName, lpString2, v1);
    if ( sub_100011CE(&FileName, (WCHAR *)&v5) )
    {
      v2 = ((int (__thiscall *)(int, signed int))SetErrorMode)(v4, 32775);
      sub_100010AD((int)&v5, &FileName);
      SetErrorMode(v2);
    }
  }
  return 0;
}

//----- (100010AD) --------------------------------------------------------
signed int __cdecl sub_100010AD(int a1, LPCWSTR lpFileName)
{
  signed int result; // eax@1
  int v3; // ebx@1
  int v4; // edi@2
  const void *v5; // ecx@2
```

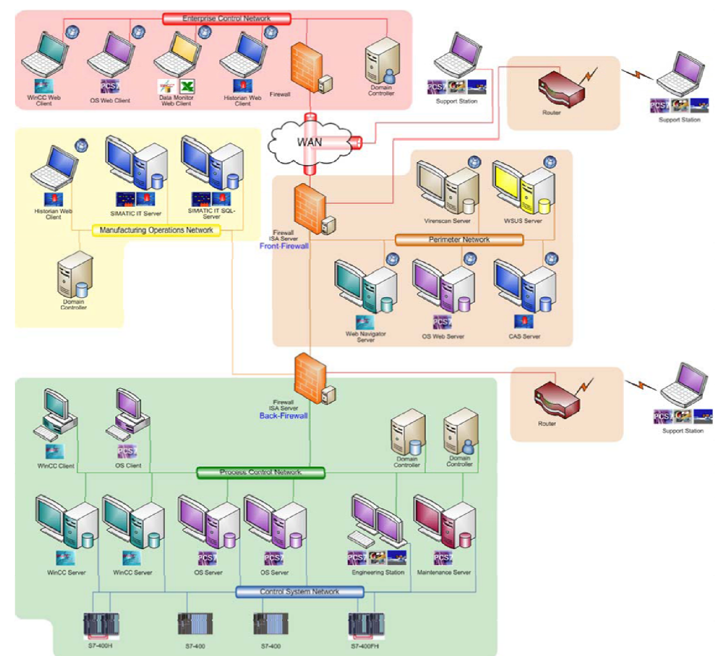


Figure 4: The Hypothetical ICS Network Architecture

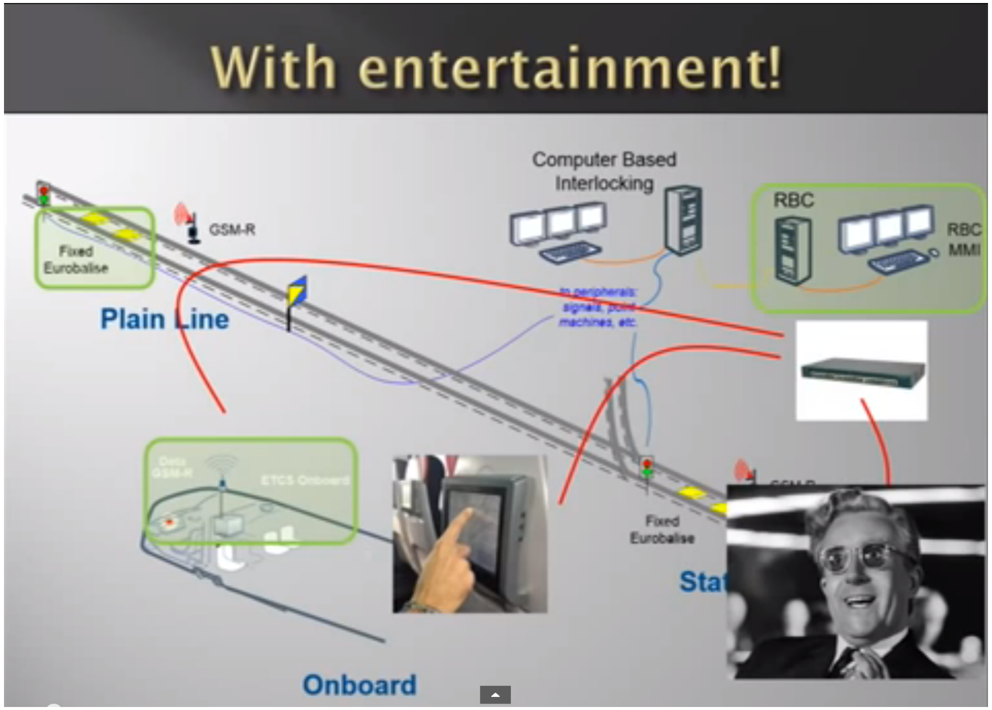
Polish teen derails tram after hacking train network (Jan 2008)

- *"A Polish teenager allegedly turned the tram system in the city of Lodz into his own personal train set, triggering chaos and derailing four vehicles [...]*
- *The 14-year-old modified a TV remote control so that it could be used to change track points [...]*
- *Twelve people were injured in one of the incidents:*
  - *"It was lucky nobody was killed. Four trams were derailed, and others had to make emergency stops that left passengers hurt. He clearly did not think about the consequences of his actions"*
- *The youth, described by his teachers as an electronics buff and exemplary student, faces charges of endangering public safety"*

http://www.theregister.co.uk/2008/01/11/tram_hack/

Signaling and entertainment

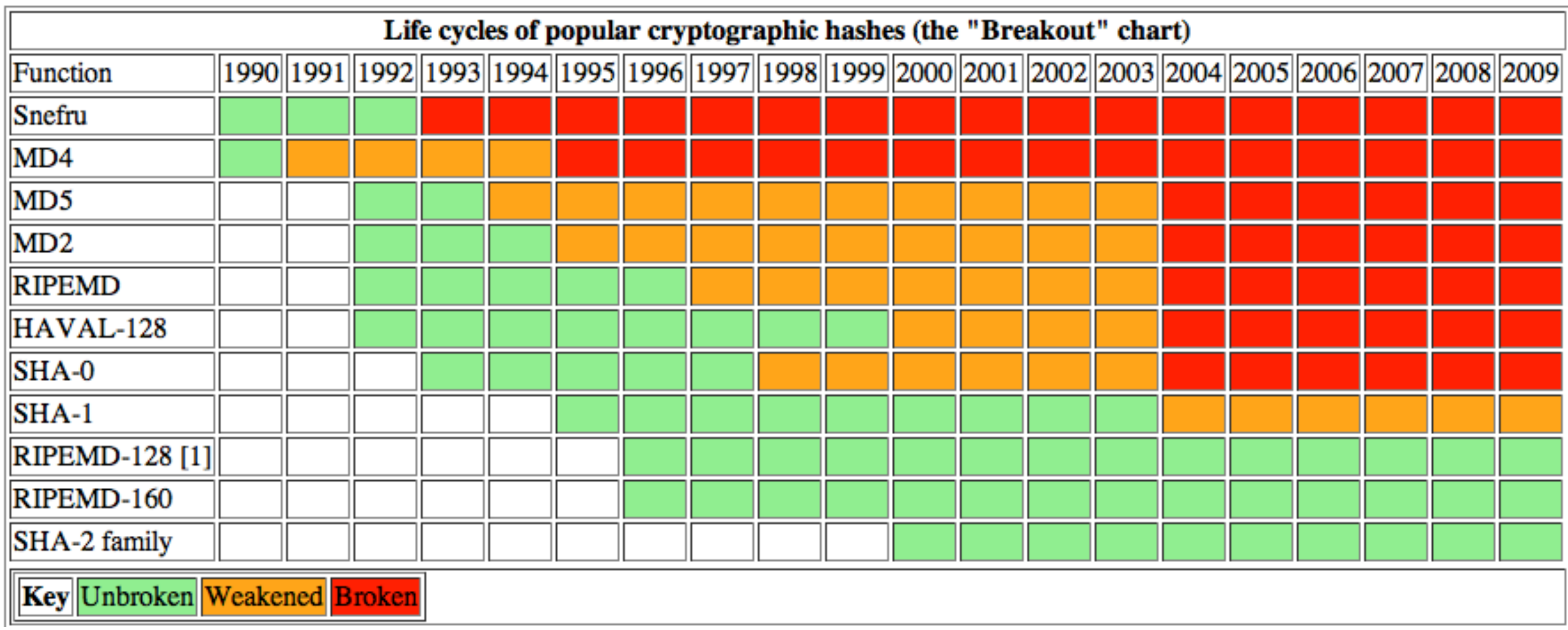
http://scadastrangelove.blogspot.it/search/label/Releases



2013 Chaos Club https://youtube.googleapis.com/v/2-kFlIWpCGg
%26source=uds

http://www.shodanhq.com/

Mechanisms degrade - life time of cryptographic hashes



"The code monkey's guide to cryptographic hashes for content-based addressing"
http://valerieaurora.org/monkey.html

Gsm security – a timeline

1987 – A5/1 cipher developed, details kept secret

1994 – General design of A5/1 leaked, first attacks published

1999 – A5/1 completely reverse engineered

2000 – 130 million customers rely on A5/1 for confidentiality

2003 – Serious weaknesses identified in A5/1

2004 – J. Quirke, "Security in the GSM System", AusMobile

2005 – GSM accounts for 75% of the worldwide cellular market

2006 – "Instant Ciphertext-only Cryptanalysis of GSM Encryption"

2009 – A5/1 Cracking project launched (July), succeeded (Dec)

2009 – "Practical complexities underestimated", GSM Association

2010 – "Breaking GSM Security with a $15 phone", CCC 2010

2012 – "GSM-R is a robust and secure system", Network Rail

Messages

- Security degrades with time
  - Attack tools improve
- Attack focus changes with time
- Wide variation in attack sophistication

The nature of the systems

- Socio-technical-political
- Multi-owner
- Multi-scale
- Complex
- Adaptive
- Evolve
- Long-lived

Power laws and fat tails

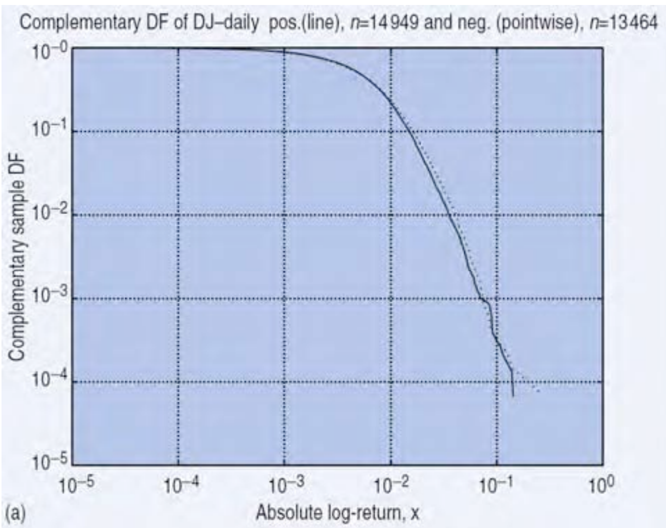
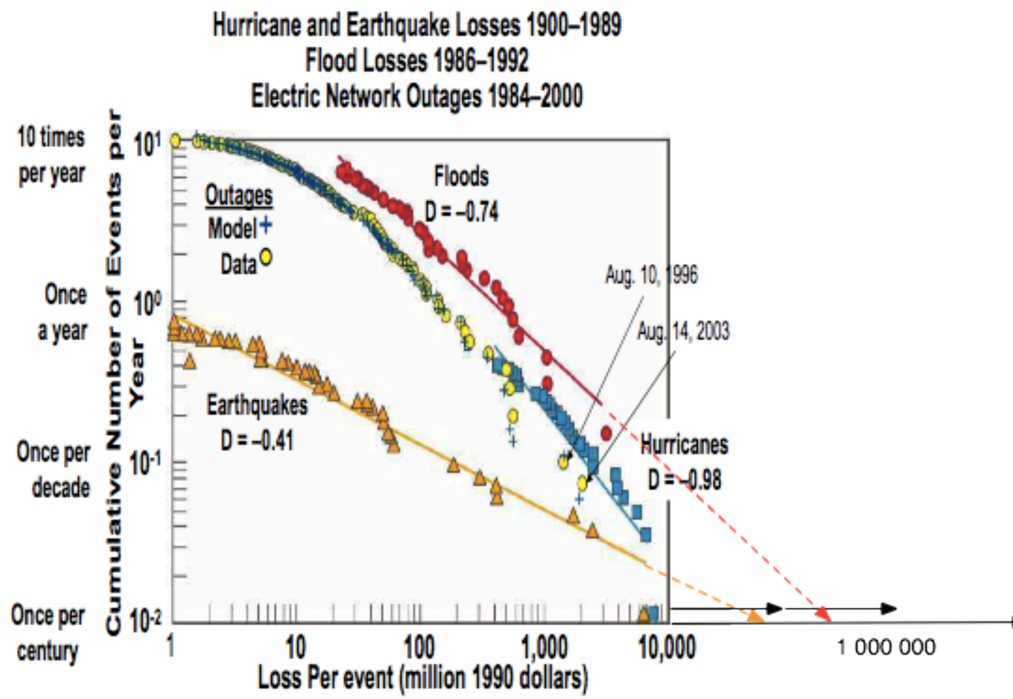
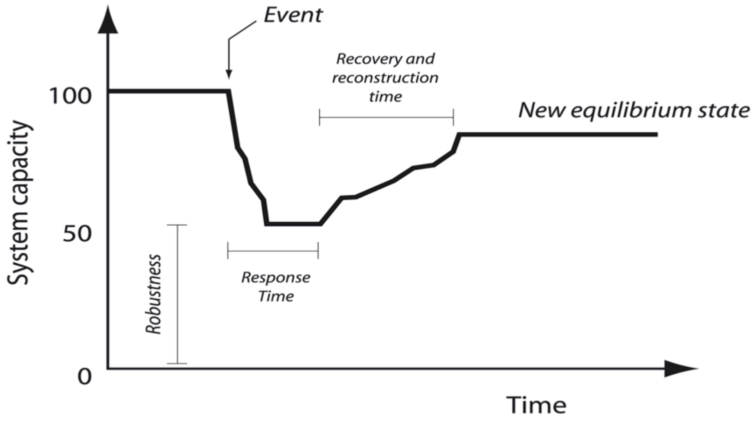


Fig.7 Survival distribution of positive (continuous line) and negative daily returns (dotted line) of the Dow Jones Industrial Average index over the time interval from May 27, 1896 to May 31, 2000, which represents a sample size of n=28 415 data points. The straight part in the tail in this log-log scale qualifies a power law distribution with exponent μ≈3. Reproduced from Malevergne et al. [8].



Visually power laws but see critiques

Importance of resilience



- Type 1: Resilience to design basis threats. This could be expressed in the usual terms of availability, robustness, etc. It could be bounded by credible worst case scenario.
- Type 2: Resilience to beyond design basis threats. This might be split into those known threats that are considered incredible or ignored for some reason and other threats that are unknowns.

•Attacks on intangibles - these are also societal assets, not just CIP

•Does addressing Type 2 help with Type 1?

Railway system analysis

Figure 4: The Hypothetical ICS Network Architecture

Layered analysis

- M0 Policy and requirements – the highest level structure where the represents the abstract security, safety, resilience policy
- M1 Abstract implementation – the abstract implementation or specification level with connectivity details abstracted
- M2 Abstract network with detailed topology
- M3 Implementation detail
- Iterative, phased approach

Overall N step process – “the 39 steps”

- The “39 steps” should include
  - Definition of impact level
  - Abstraction and layering of the system and assurance
  - **Scenarios**
  - **Factorisation of claims**
  - **Uncertainty in structure**
  - Address evolution and adaptation
  - **Monotonic arguments**
  - Identify signals
    - Precursors and indicators
  - Points of influence
  - **Embrace openness**
  - **Risk communication**
    - Explaining level of understanding

Scenarios

- Role of imagination
- Compounding risks
- Exposing implicit values and assumptions
- Explore design basis threats and events

- Narrative, interviews, incidents, field work
- Analysts
- Technical knowledge and creative insights

Attack Scenarios

- Structured analysis of each attack scenario:
  - What is the attack scenario?
  - How is the attack performed?
  - What vulnerabilities does the attack exploit?
  - Where can the attack be launched from?
  - What are the possible mitigations?
- Grading of attack scenarios (Red, Yellow, Green):
  - Level of access
  - Degree of technical sophistication
  - Scale and impact of attack
  - Difficulty of mitigation

Focus – high consequence

- Safety means system designed to be fail-stop
  - But do not equate with fail-safe
- High casualty
  - Collision, high end capability attacke
  - Compounded e.g. chlorine tanker in city
- High profile
  - Targeted individual
- Slow recovery
  - Of railway attack
  - Other incidents compounded
- Availability, integrity rather than confidentiality
  - Except for learning, Royal trains, nuclear waste
  - Attacks on confidence

Overall N step process – “the 39 steps”

- The “39 steps” to include
  - Definition of impact level
  - Abstraction and layering of the system and assurance
  - **Scenarios**
  - **Factorisation of claims**
  - **Uncertainty in structure**
  - Address evolution and adaptation
  - **Monotonic arguments**
  - Identify signals
    - Precursors and indicators
  - Points of influence
  - **Embrace openness**
  - **Risk communication**
    - Explaining level of understanding

Factorisation

- P(Consequence) = P(Consequence | attack) P(attack)
- Capabilities
  - Categorise attacks by capabilities
  - Leaves likelihood of threat for others to assess
  - Does not "hard-wire" into analyses
- Push assumptions into left hand side
  - P(Consequence | attack, assumptions…)
- Output becomes more conditional
  - But might clash with wish to compare risk
  - Sensitivity studies on threat assumptions across different types of risks

Overall N step process – "the 39 steps"

- The "39 steps" to include
  - Definition of impact level
  - Abstraction and layering of the system and assurance
  - **Scenarios**
  - **Factorisation of claims**
  - **Uncertainty in structure**
  - Address evolution and adaptation
  - **Monotonic arguments**
  - Identify signals
    - Precursors and indicators
  - Points of influence
  - **Embrace openness**
  - **Risk communication**
    - Explaining level of understanding

The myth of air gaps

- Mr. MCGURK *In our experience, in conducting hundreds of vulnerability assessments in the private sector, in no case have we ever found the operations network, the SCADA sys- tem or energy management system separated from the Enterprise network. On average, we see 11 direct connections between those networks and in some extreme cases, we have identified up to 250 connections between the actual producing network and the enterprise environment.*

CYBERSECURITY: ASSESSING THE IMMEDIATE THREAT TO THE UNITED STATES

HEARING

BEFORE THE

SUBCOMMITTEE ON NATIONAL SECURITY, HOMELAND DEFENSE AND FOREIGN OPERATIONS

OF THE

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED TWELFTH CONGRESS

FIRST SESSION

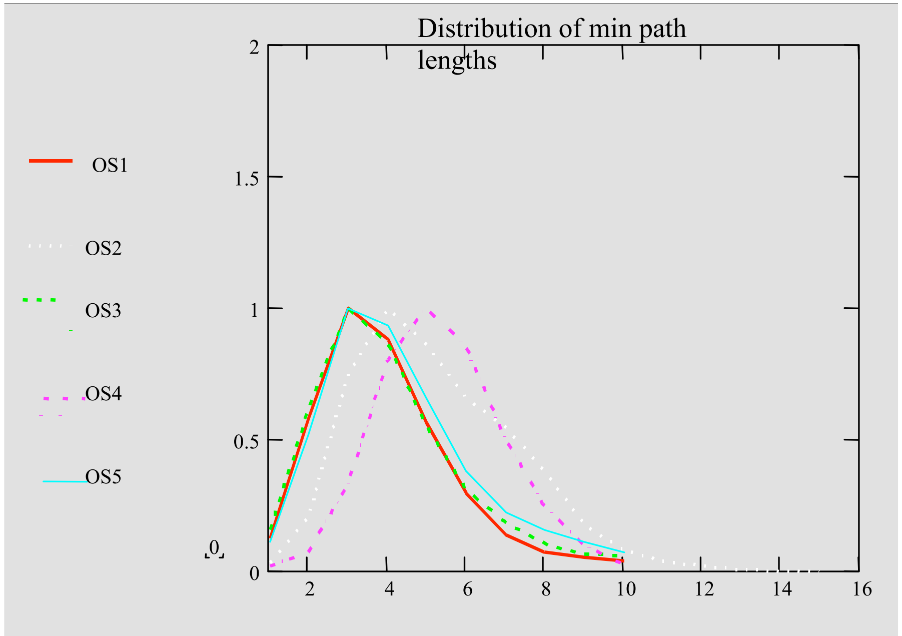
MAY 25, 2011

Serial No. 112–55

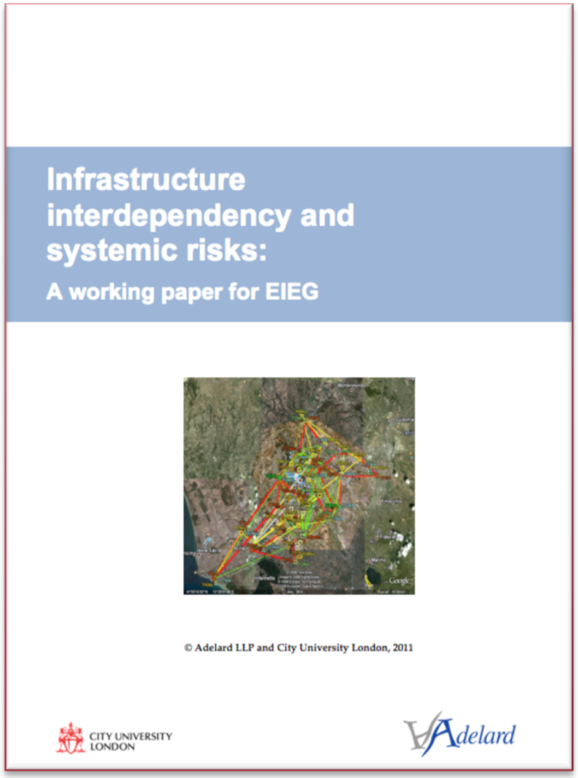
Printed for the use of the Committee on Oversight and Government Reform

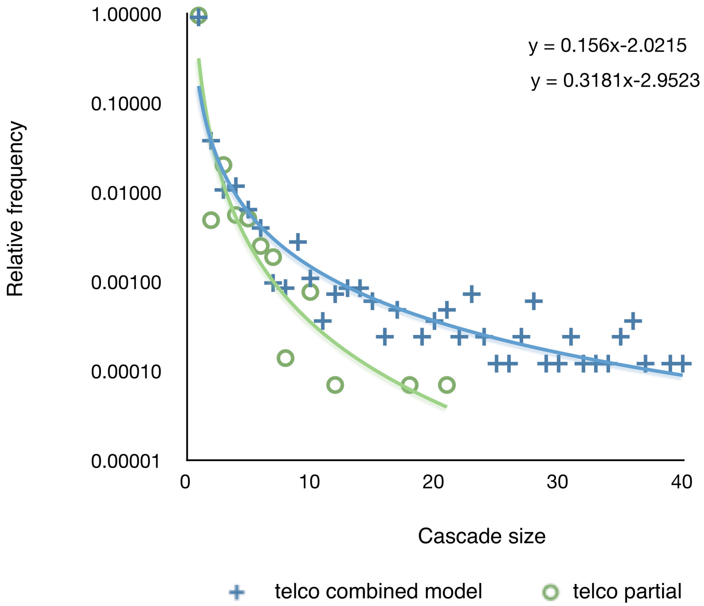
Address uncertainty in structure

- Connectivity
  - Well known small world results
  - Industrial software examples



Critical infrastructure interdependencies





Layered analysis

- Levels of abstraction:
- M0 Policy and requirements – the highest level structure where the represents the abstract security, safety, resilience policy
- M1 Abstract implementation – the abstract implementation level with connectivity details abstracted
- M2 Abstract network with connectivity
- M3 Implementation

Analysis at different abstraction levels

Uncertainty in structure	Approach	Output/benefits
M0 Policy and requirements – the highest level structure where the represents the abstract security, safety, resilience policy	Overall statements about uncertainty; caution in claims	Shaping expectation and system design; design basis threats; ; defence in depth princples
M1 Abstract implementation – the abstract implementation level with connectivity details abstracted	Increased impact of failures, distribution of size of events via general laws	More realistic estimate of loss and attack surface
M2 Abstract network with connectivity	Network based probabilistic models, topological analysis	Sensitivity of design, identification of critical components, identification of responsibilities and dependencies
M3 Implementation in detail	As above with more detail; results of actual PEN tests	Operational risk Procedures and mitigations

Overall N step process – "the 39 steps"

- The "39 steps" to include
  - Definition of impact level
  - **Scenarios**
  - **Factorisation of claims**
  - **Uncertainty in structure**
  - Address evolution and adaptation
  - **Monotonic arguments**
  - Identify signals
    - Precursors and indicators
  - Points of influence
  - **Abstraction and layering of the system and assurance**
  - **Embrace openness**
  - **Risk communication**
    - Explaining level of understanding
- Iterative, phased approach

Embrace openness - design for open assurance

- What should be exposed
  - Principles of openness
    - Democratisation of assurance
    - Open Government
  - Balance of risks approach
    - Technocratic
- Inevitable
  - Forced openness
  - Threat assumptions
- How to act on results
  - Wisdom of clouds vs tyranny of the many

Some outputs from risk assessment

- Fundamental responsibility
  - Understand and communicate hazards and their mitigation
- Understanding of the types of risks
  - Discuss values and tolerability
- Analysis and discussion of design and risk trade-offs
  - or a basis for this
- Principles for network design
  - Good and bad things, critical issues
- Assurance options and focus
  - Structural uncertainties and impact, openness
- Signals to monitor adaptation and change
- An estimate of the risk

Discussion

- Risk assessment provides many useful outputs
  - an estimate of the risk is ~~not~~/only one of them
- Fundamental responsibility
  - Understand hazards and their mitigation
  - Communicate the nature of risks and resilience

SESAMO project

Security and Safety Modelling
for embedded systems
14 companies and 6 research institutes
in Europe and the U.S.

http://sesamo-project.eu/

Objectives include:

- joint reasoning about safety and security properties, conflicts and synergies
- a model-based methodology and solutions for addressing safety and security within an integrated process, supported by an effective tool chain
- validation in use cases in multiple industrial domains (e.g. aerospace, energy management, automotive, metropolitan rail and mobile medical)

ADELARD