CIR Risk Management AWARDS 2014 winner

Risk Management Specialist Company of the Year

CRA risk analysis

Digital C&I Reliability

Hugh Stephenson, Principal Consultant, CRA

CRA Risk Forum, 6th October 2016

CRA risk analysis

IOP Institute of Physics Awards 2015

Winner! Best Practice in Professional Development

crarisk.com

Contents

1) A problem close to home
2) Increasing use of digital C&I in NPPs
3) Digital C&I applications in NPPs
4) Current approaches to reliability estimation of digital C&I
5) Problems with current approaches
6) Possible approaches looking forwards
7) Cyber security impacts on nuclear safety

"Oh, it always does that. Just turn it off and on again."
Everyone, 1990 onwards

A problem close to home

- #1: Moto GP Round 6 – Mugello, Italy, May 2016

Jorge Lorenzo was first to suffer a problem, in morning warm-up, with factory team-mate Valentino Rossi then forced to retire from his home event in a cloud of smoke while shadowing Lorenzo for the race lead.

A CCF event in MotoGP?

"…neither an engine component nor a structural failure, **it was purely an electronic control issue**. "

"We have a strong history of engine reliability and this fact does not change after this incident; the engines had no problems, but **we were not aware of the different behaviour of the standard ECU software, that made the rev limiter work in a different way compared to last year. We set the rev limiter using last year's data in exactly the same way as we did last year, but we could not be aware that the software worked in a different way."**

Kouji Tsuya, Yamaha YZR-M1 Project Leader

A problem close to home

- #2: My 1995 Mitsubishi FTO failure, Air balloon roundabout, Gloucester, April 2016

The Technology

- INVECS (Intelligent & Innovative Vehicle Electronic Control System)
- Tiptronic gearbox control c. 1994 fully automatic / clutchless semi-automatic
- Adaptive Shift Control software which monitored and "learned" the driver's habits over time and adjusted the smoothness or aggression of the gearshifts to suit his or her driving style. (In 1994!)

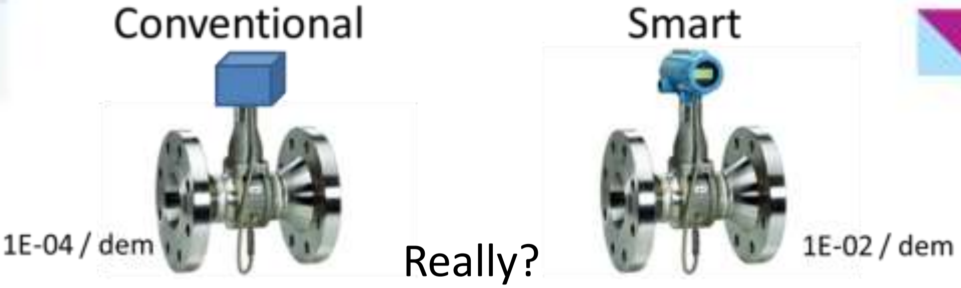
The Failure

- Infrequent fluid changes resulted in metal particle build up on gearbox input and output shaft speed sensors
- Software no longer had required inputs from sensors - control system failure
- Bypass valve opened to allow ‘limp home’ in 3rd gear through the traditional torque converter
- Car now converted to manual gearbox complete with human operated clutch… 😉

Increasing use of Digital C&I in NPPs

- Why?

- Both in existing and new plants



- Aging and obsolescence

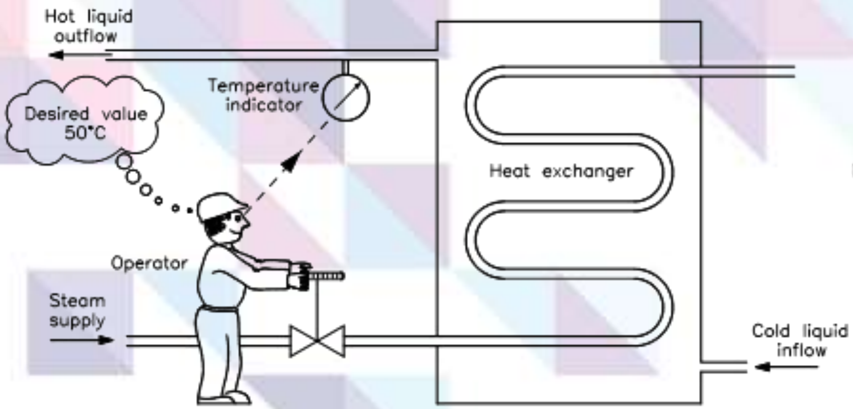
- Improved control and functionality (e.g. condition monitoring)

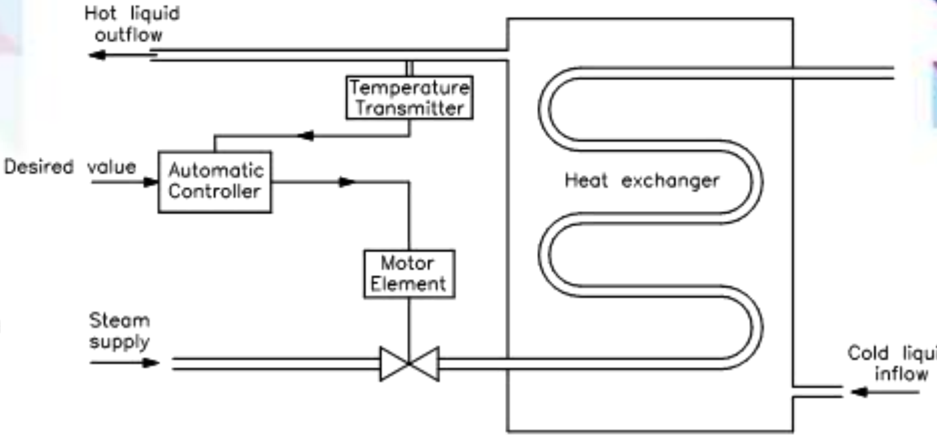
- Make our lives and tasks easier and more efficient

- Because we can! A ‘tech happy’ generation with cheap digital equipment available and in use across many industries

Automation in NPP

- Comparisons with manual control





Failure to provide hot liquid outflow:

- Indication failure (analogue) +
- Operator failure (HEP) +
- Valve failure (mechanical)
- Minimal dependencies (electrical, HVAC etc.)

Failure to provide hot liquid outflow:

- Temp sensor/transmitter failure +
- Automatic controller failure +
  (hardware & software (HEP?)), SMART?
- Telemetry failure +
- Valve actuator failure +
- Valve failure (mechanical)
- Many dependencies (electrical, HVAC etc.)

Which is likely to be more reliable? What's the uncertainty?

Digital C&I application at NPPs

- 'Duty' functions such as process control

- Process Control System (PCS) functions include:
  - Deaerator level control
  - Condenser level control
  - MSR Reheat Temperature and Pressure Control
  - Let down temp and press control, Etc.
- Most are effectively 'continuously running' during normal operation
- Safe and dangerous failures - in what context?
- Failures could result in transients leading to initiating events (e.g. unplanned reactor trip - turbine trip, loss of feed)
- Reliability and availability both of interest for safety and commercial reasons
- Typically interested in failures per time, **usually per annum**
- Comparison with 'targets' , in turn often driven by safety cat/class but for what? Component /system failure? Functional failure?

Digital C&I application at NPPs

- 'Standby' functions to protect plant and ensure nuclear safety

- NPP employ many redundant and standby safety systems
  - Standby feed pump auto start
  - Diesel Generator inc. Auto Voltage Regulator
  - Turbine protection (over speed, negative phase protection)
- Use of COTS, sometimes application differs.
- Again, mixture of digital and analogue equipment
- Are effectively 'on standby' and are not running during normal operation, but may include continuous monitoring of running plant.
- Failures could result in failure of a safety function post initiating event, or propagation of an initiating event
- Typically interested in **failures per demand** with low number of demands per year

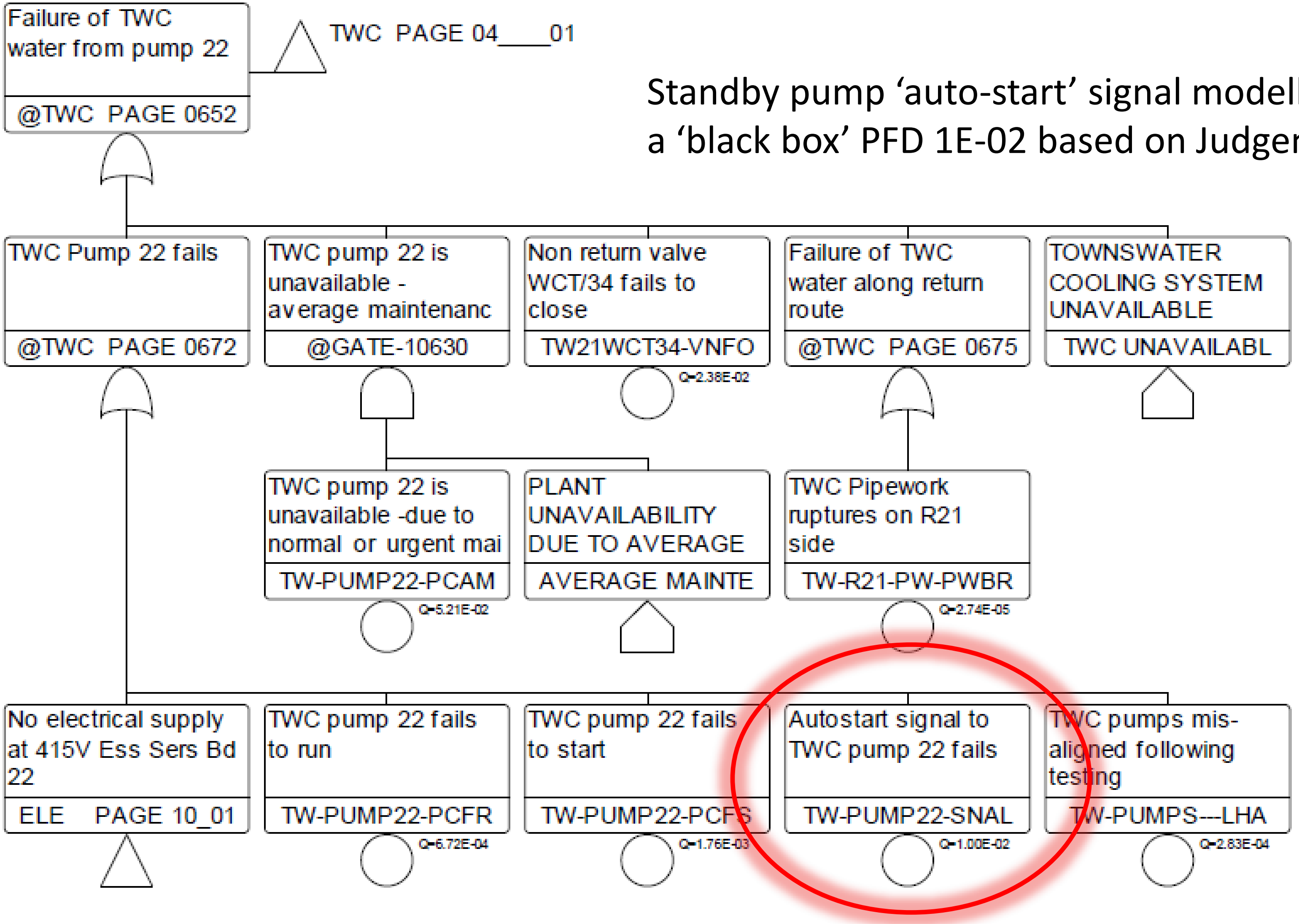
Current approaches to reliability estimation

- Overview

- Varies depending on C&I – large process control/reactor protection cf. SMART
- Varies depending on industry and even utility within each industry
- Usually some consideration of digital C&I failure in PSA and safety cases, increased focus – appropriate?
- Level of detail depends on complexity of C&I and when it was modelled
- Software reliability estimation remains problematic, conservative values often used
- Hardware reliability , including CCF, important but need to model at an appropriate level of detail (‘compact model’)

Current approaches to reliability estimation

- The ‘black box’



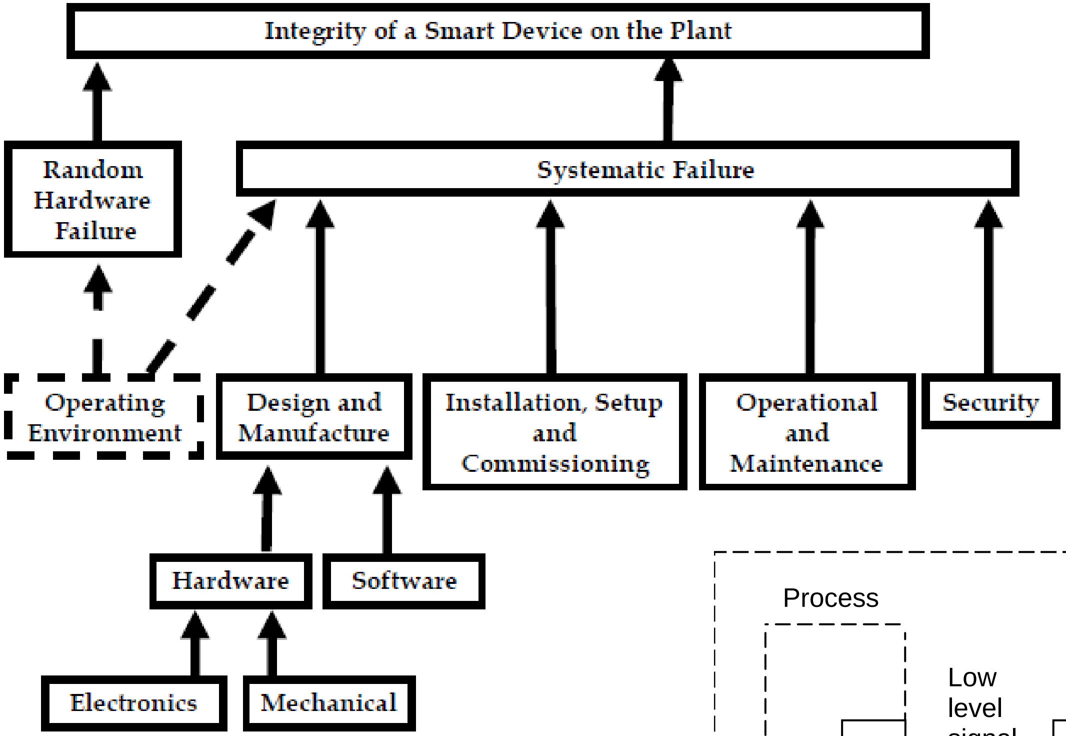
Failure of TWC water from pump 22
@TWC PAGE 0652
TWC PAGE 04___01
TWC Pump 22 fails
@TWC PAGE 0672
TWC pump 22 is unavailable - average maintenanc
@GATE-10630
Non return valve WCT/34 fails to close
TW21WCT34-VNFO
Q=2.38E-02
Failure of TWC water along return route
@TWC PAGE 0675
TOWNSWATER COOLING SYSTEM UNAVAILABLE
TWC UNAVAILABL
TWC pump 22 is unavailable -due to normal or urgent mai
TW-PUMP22-PCAM
Q=5.21E-02
PLANT UNAVAILABILITY DUE TO AVERAGE
AVERAGE MAINTE
TWC Pipework ruptures on R21 side
TW-R21-PW-PWBR
Q=2.74E-05
No electrical supply at 415V Ess Sers Bd 22
ELE PAGE 10_01
TWC pump 22 fails to run
TW-PUMP22-PCFR
Q=6.72E-04
TWC pump 22 fails to start
TW-PUMP22-PCFS
Q=1.76E-03
Autostart signal to TWC pump 22 fails
TW-PUMP22-SNAL
Q=1.00E-02
TWC pumps mis-aligned following testing
TW-PUMPS---LHA
Q=2.83E-04

Standby pump ‘auto-start’ signal modelled as a ‘black box’ PFD 1E-02 based on Judgement

Current approaches to reliability estimation

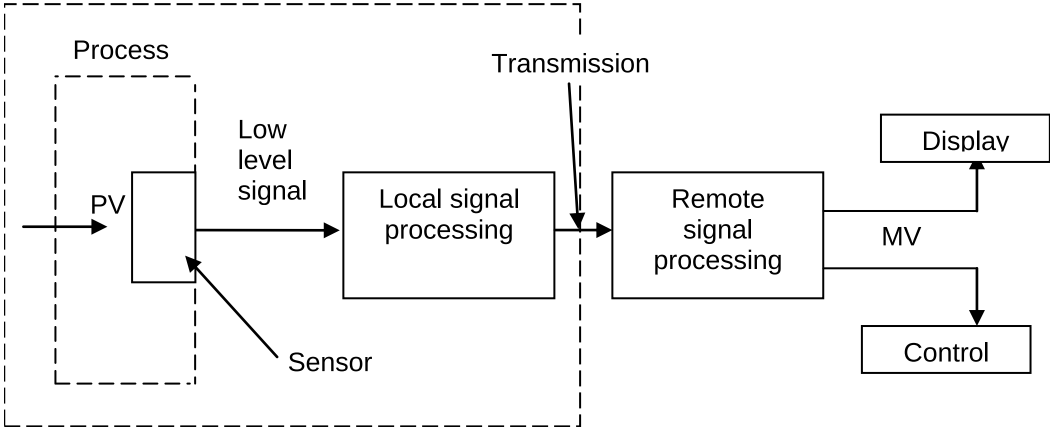
- Digital C&I Failure Modes

SMART component



Process control

Transmitter



Current approaches to reliability estimation

- Software reliability

- Excludes consideration of hardware/memory failure induced software failure – so this should be considered separately. Is it?

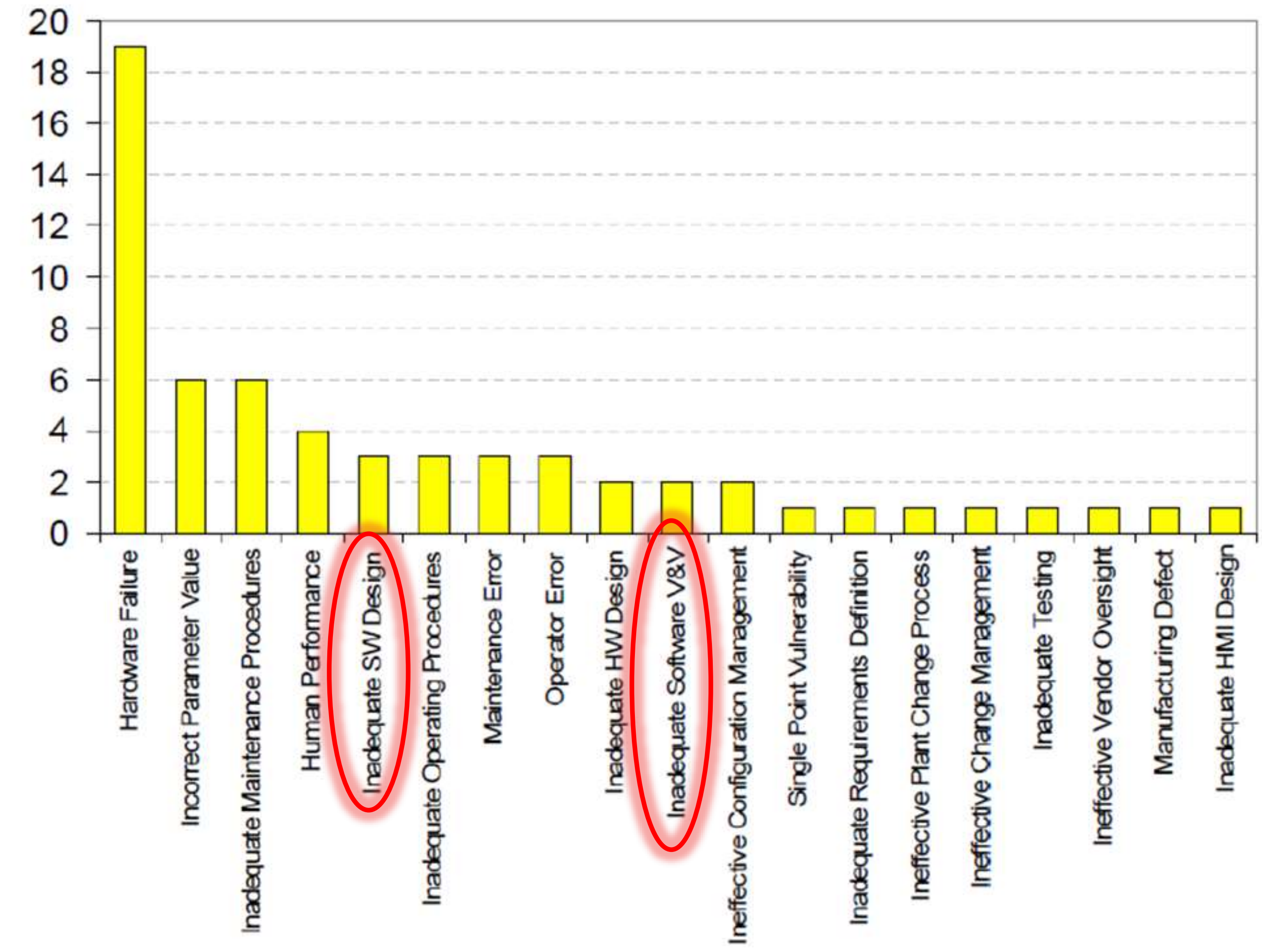
- Level of effort increases significantly as integrity target increases

- 2 legged' qualitative approach used currently
  - Production Excellence assessment
  - Independent confidence building measures (ICBM)

- Output of assessment often used in PSA models as input to 'Black Box' – but is this appropriate?

But is software really a problem?

- Taking a look at the OPEX



Problems with current approaches

- Overview

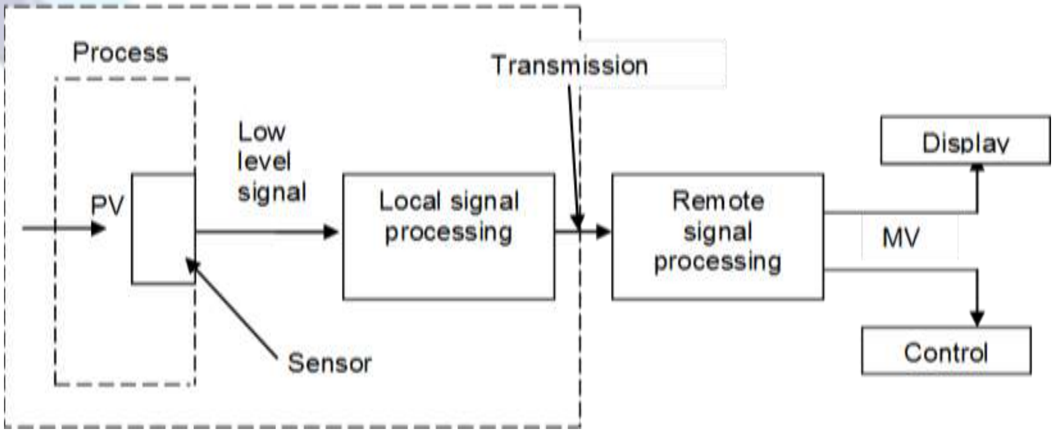
- Majority of other data in PSA is **Best Estimate**
- *……. it refers to the most accurate value of the data item derived from experiment, operating experience, judgement etc. as appropriate. Where there is inadequate evidence, and no credible best estimate is possible, then bounding or conservative values should be used"* (ONR)

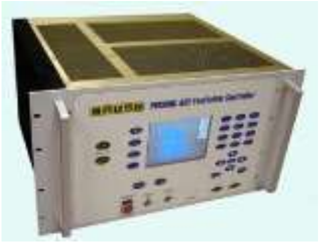
- In PSA for most random failures, an estimate of the mean is typically used as the best estimate. Increasing use of Bayesian approaches.
- Use of conservative 'target' numbers can completely dominate results, skewing numerical risk predictions and generating misleading risk insights
- Concern that other more prominent mechanical, electrical and human failures are overlooked
- The model also provides little or no insights as to the likely causes of the C&I failure. As a result, difficult to use the model for risk informed design and optimisation

Problems with current approaches

- The Good, the Bad and the Ugly

- Inconsistent approaches adopted in modelling depending on ‘need’
- Inappropriate ‘bounding’ by other conditional probabilities
- Functional boundary issues – what if multiple digital I&C components are required to perform a function?





crarisk.com

Problems with current approaches

- The Good, the Bad and the Ugly

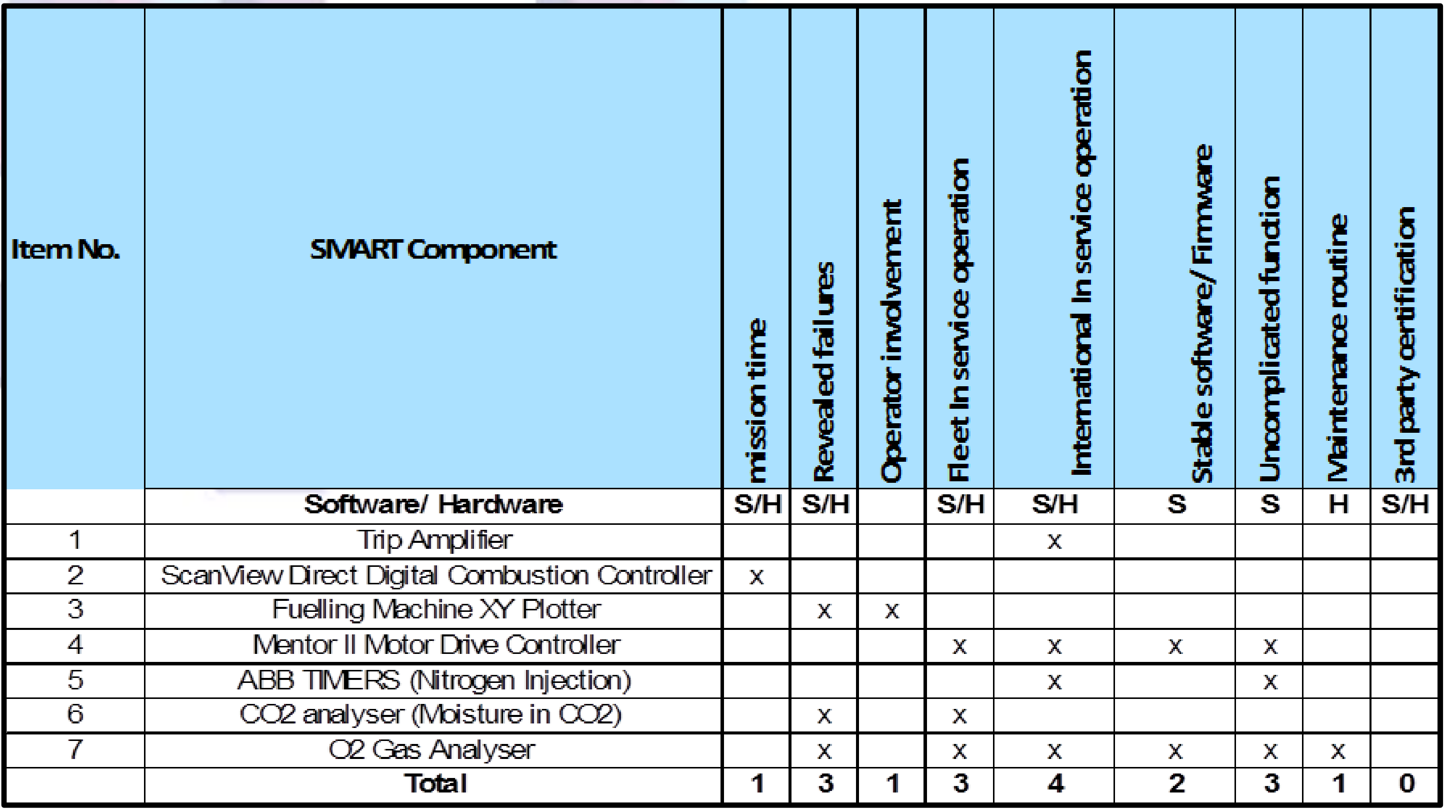
- Complete omission due to lack of awareness or replacement with ‘like for like’ - but not quite as new one looks the same but is in fact digital!

- Treatment of systematic failures (hardware (CCF) and software) - Inter functional systematic failures not generally considered.

- Focus of failure - spurious operation often not considered. Time consuming and labour intensive.

Possible ways forward

- Requirement to produce ‘best estimate’ data and guidance for PSA / Safety Case

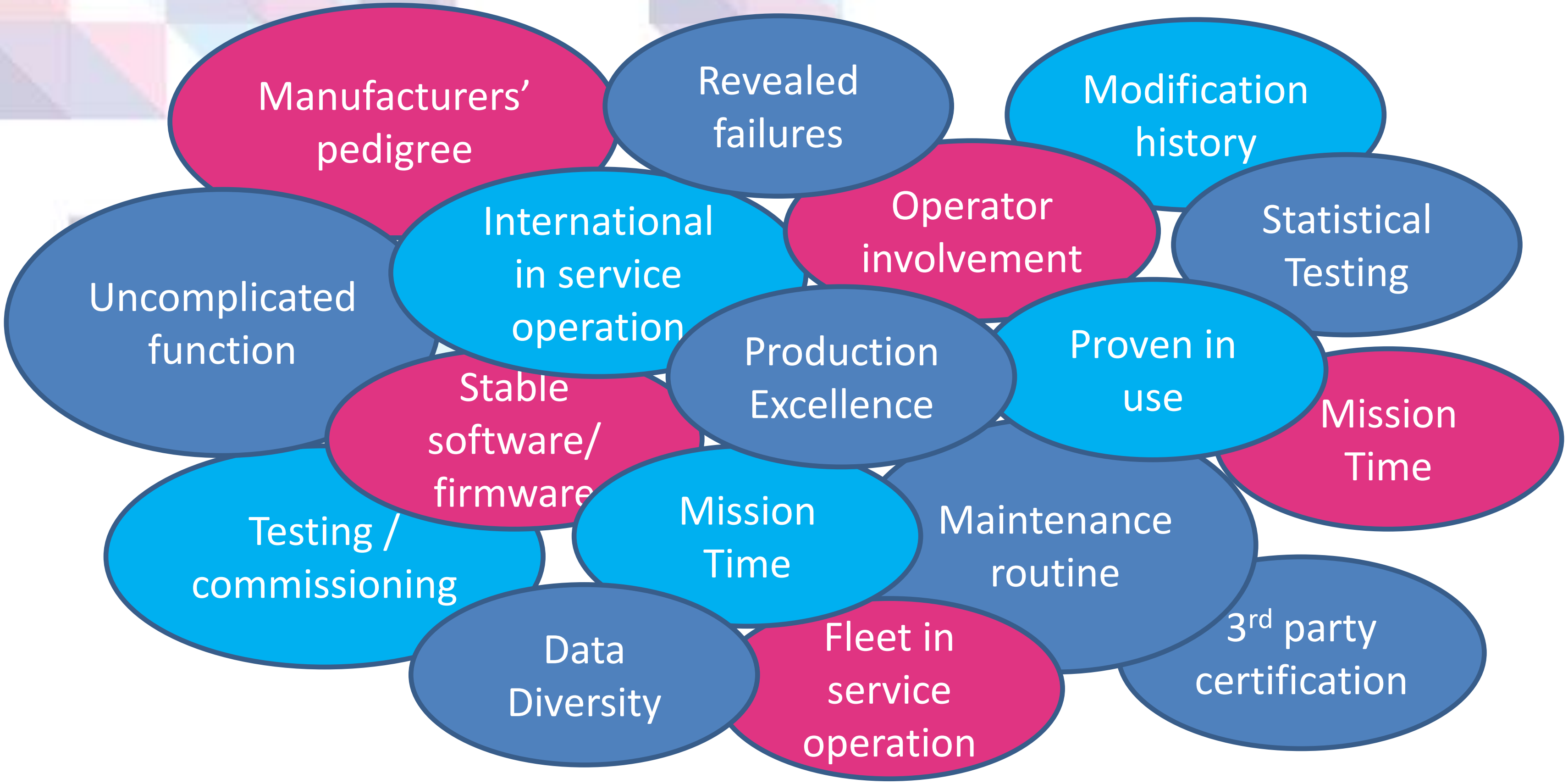


Item No.	SMART Component	mission time	Revealed failures	Operator involvement	Fleet In service operation	International In service operation	Stable software/ Firmware	Uncomplicated function	Maintenance routine	3rd party certification
	Software/ Hardware	S/H	S/H		S/H	S/H	S	S	H	S/H
1	Trip Amplifier					x				
2	ScanView Direct Digital Combustion Controller	x								
3	Fuelling Machine XY Plotter		x	x						
4	Mentor II Motor Drive Controller				x	x	x	x		
5	ABB TIMERS (Nitrogen Injection)					x		x		
6	CO2 analyser (Moisture in CO2)		x		x					
7	O2 Gas Analyser		x		x	x	x	x	x	
	Total	1	3	1	3	4	2	3	1	0

- What is the overlap between Production Excellence, ICBMs and the additional arguments being made?
- While the qualitative arguments are sound, the reduction in reliability value seems to be arbitrary (often x 0.1).

Possible ways forward

- Arguments to further reduce software unreliability claims



Manufacturers' pedigree

Revealed failures

Modification history

Operator involvement

Statistical Testing

Uncomplicated function

International in service operation

Production Excellence

Proven in use

Mission Time

Stable software/ firmware

Testing / commissioning

Mission Time

Maintenance routine

3rd party certification

Data Diversity

Fleet in service operation

Guidance? Framework? Expert Judgement?

Impact of cyber security on reliability

- Overview

- Security and safety historically separate in industry.
- ONR SyAPS (Security Assessment Principles) released in 2016 to augment well established ONR SAPs
- Strong views that having a strong nuclear safety culture will not ensure that you are ‘nuclear secure’. However, of more interest to safety community is consideration of **how security shortfalls could affect nuclear safety. How much risk is missing and should this be more visible?**
- Need to improve communication between nuclear safety and security
- Inaugural Nuclear Cyber Security & Safety working group chaired by CRA in July 2016.
- Need to consider carefully software updates /patches to improve security given previous production excellence on earlier versions i.e. never, following careful review of code changes, automatic?

Impact of cyber security on reliability

- #1 - STUXNET

- Malicious computer worm believed to be a jointly developed US/Israeli Cyber weapon - reportedly ruined almost one fifth of Iran's nuclear centrifuges

- Targets PLCs - via Windows and Siemens Step 7 software - which allow the automation of electromechanical processes such as those used to control machinery on factory assembly lines, amusement rides, or centrifuges for separating nuclear material

- Could be tailored as a platform for attacking modern SCADA and PLC systems (e.g., in automobile or power plants).

- Typically introduced via a USB flash drive, modifies the software codes and **gives unexpected commands to the PLC while returning a loop of normal operations system values feedback to the users. I.e. dangerous undetected failures**

- What impact on risk could a similar attack have on an operating NPP?
- Should we try to quantify it?

Impact of cyber security on reliability

- #2 - Loss of Grid in Ukraine, December 2015

- On December 23, 2015, the Ukrainian Kyivoblenergo, a regional electricity distribution company, reported service outages due to a third party's illegal entry into the company's computer and SCADA systems: Starting at approximately 3:35 p.m. local time, seven 110 kV and 23 35kV substations were disconnected for three hours.

- Ukrainian government officials claimed the outages were caused by a **cyber attack**, and that Russian security services were responsible for the incidents.

- Currently consider Loss of Offsite Power as an IE in NPP PSA models and for some designs this is particularly risk significant

Short (<2h) LOOP	~5E-02/yr (i.e. once every 20 years)
Long (2-24 hours) LOOP	~5E-03/yr (i.e. once every 200 years)

- Main contributor (only for Long LOOP) is high wind hazards

- Should we be now considering Cyber attacks in IEF derivation?

CRA

risk analysis

CRA is a diverse, specialist risk analysis consultancy employing a multi-disciplined team to service the requirements of the safety and mission critical industries.

crarisk.com