Dealing with uncertainty

Mirek Generowicz
I&E Systems Pty Ltd - Australia

Engineers put trust in calculations

We have been calculating the probability of failure for safety functions for many years

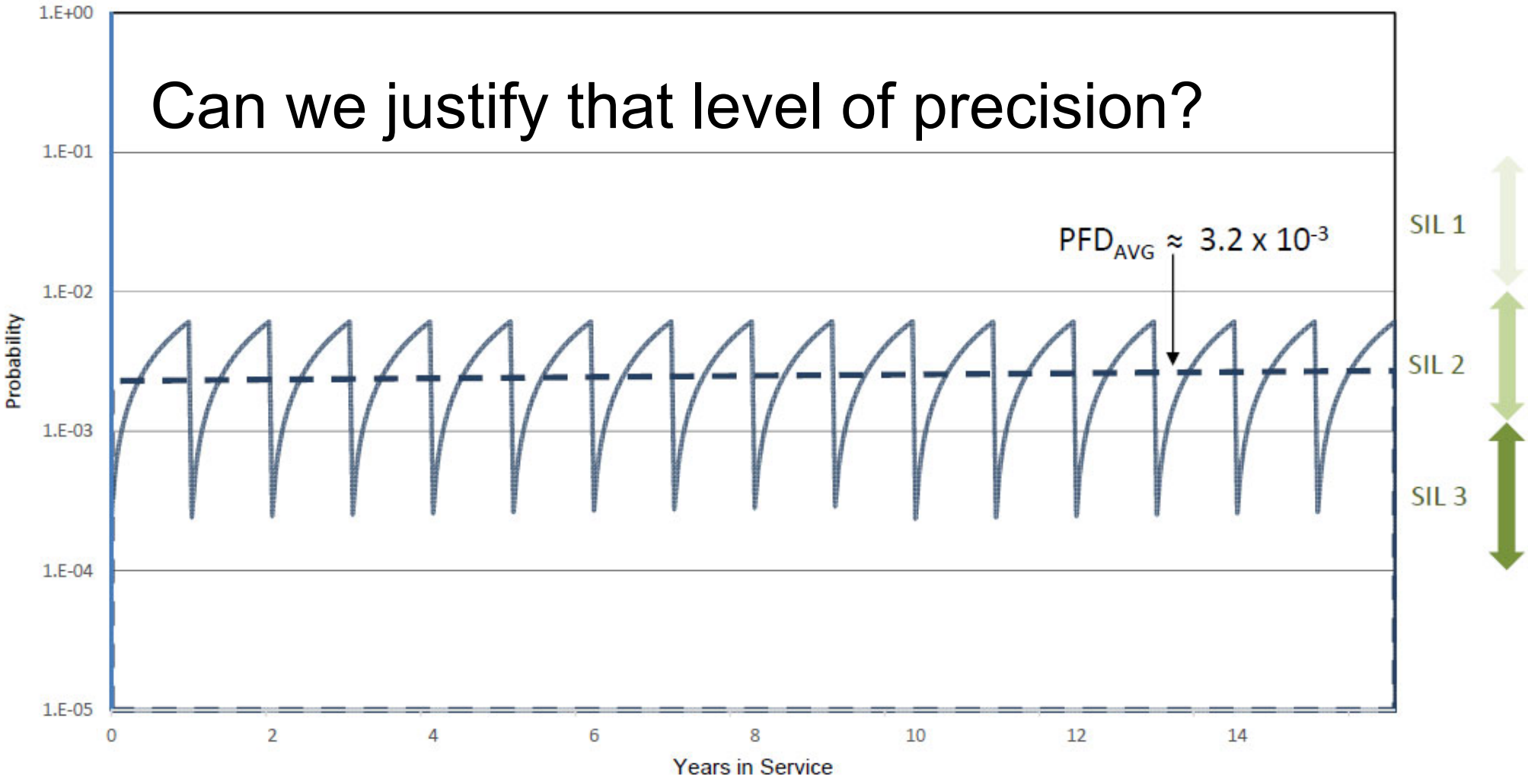
Calculation results are presented confidently with precision:

$PFD_{AVG} \approx 3.15 \times 10^{-3}$ and RRF ≈ 317

Sophisticated software shows us precisely how probability of failure will vary over time

SYSTEMS

Probability of SIF Failure on Demand



We have a challenge:

IEC 61511-1 Edition 2 added a new requirement, sub-clause 11.9.4:

> *'reliability data **uncertainties** shall be assessed and taken into account when calculating the failure measure'*

and sub-clause 11.4.9 requires that:

> *'reliability data used in the calculation of failure measure shall be determined by an upper bound **statistical confidence limit of no less than 70%**'*

What does that mean in practice?

What uncertainty should we expect in reliability data?

How can we take that uncertainty into account?

SYSTEMS

Measuring failure rate – the theory

Random failures have a **fixed and constant failure rate**

If a failure rate is reasonably constant, then the failure rate can be estimated from the **mean time between failures**:

$$\lambda \approx 1/\ \text{MTBF}$$

Mean time to failure (MTTF) may be used rather than MTBF, the difference is academic

SYSTEMS

Usage of MTBF and MTTF varies between references

IEC 61508-6 and ISO 14224 have:

MTTF = 1 / λ = τ/n, assuming repairs are 'as good as new'

MTBF = MTTF + MTTR ≈ MTTF

MTTR = Mean time to restoration

n = Number of failures observed

τ = Aggregated time in service over which the failures were observed

λ = Failure rate - **valid for constant failure rate only**

ISO 14224 defines failure rate as the conditional probability per unit of time that the item fails between t and dt, provided it has been working over [0,t]

SYSTEMS

Time between failures follows a normal distribution

The time to failure of ***individual*** devices follows an exponential distribution if the failure events are **purely independent and random**

The time between failures measured in the overall population approximates a normal distribution around the MTBF

If that is valid, then a **chi-square function** can be used to estimate the true value of a failure rate λ with any desired level of confidence from the number of failures recorded

SYSTEMS

λ can be estimated from any number of failures

The chi-square function uses only

- Number of failures
- Total time in service (device-hours)

$$\lambda_\alpha = \frac{\chi^2(\alpha, \nu)}{2T}$$

χ^2 = chi-squared function

α = 1- confidence level

ν = degrees of freedom, in this case = 2.(n + 1)

n = the number of failures in the given time period

T = the number of device-years or device-hours,
i.e. the number of devices multiplied by the given time period

SYSTEMS

Confidence levels and intervals from chi-square

- If an estimate is at the 70% **confidence level** there is a 30% chance that the true long term λ_{AVG} will be worse (higher) than the estimate $\lambda_{70\%}$

- We can define a **confidence interval**:
  There is a 90% chance that the true long term λ_{AVG} will be between $\lambda_{5\%}$ and $\lambda_{95\%}$

SYSTEMS

Confidence interval width reduces with failure count

The width of a confidence interval depends only on the number of failures recorded

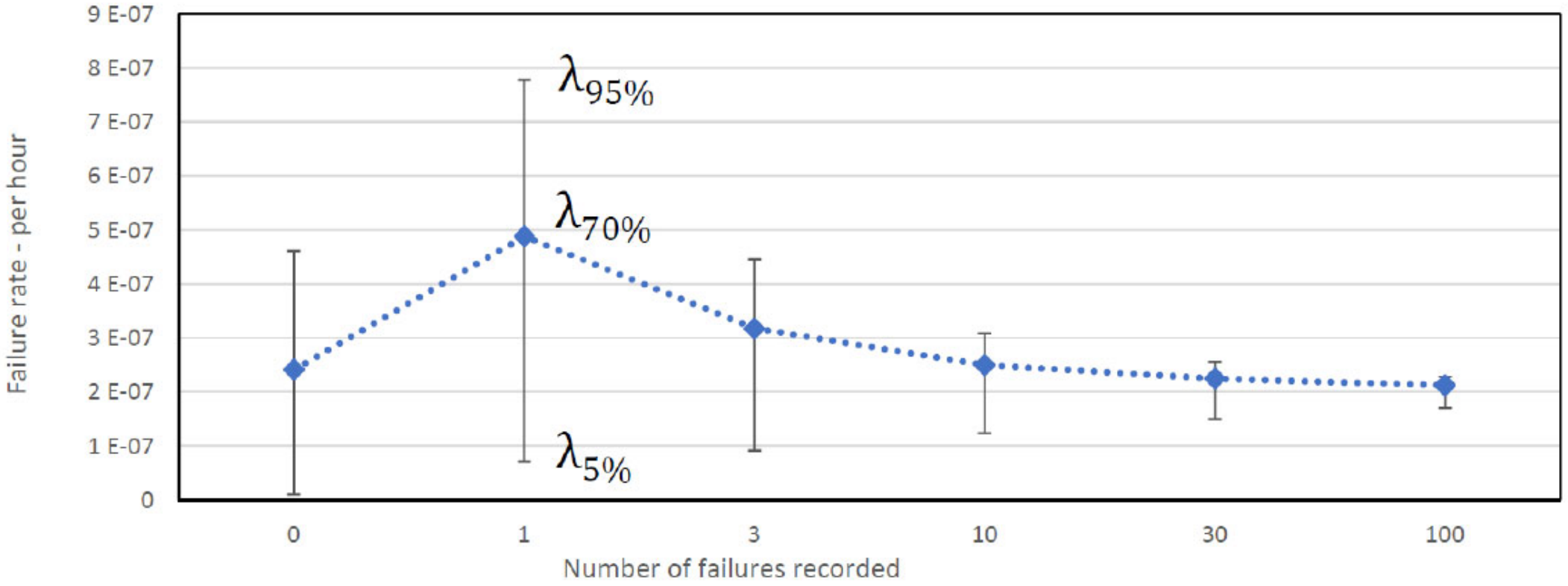
It does not depend directly on the population size

λ can even be estimated with **zero** failures, based solely on the total time in service

Confidence in the estimate of a long-term average failure rate λ_{AVG} improves as more failures are measured, i.e. the confidence interval becomes narrower

SYSTEMS

Confidence interval width reduces with failure count



SYSTEMS

But this theory does not work in practice

The chi-squared function is only valid for **purely random events** that can be characterised by a fixed and constant rate

Reality is more complicated

Few failures are purely random

We can always measure a historical average failure rate λ_{AVG} but there is no single ‘true’ constant value to be measured

SYSTEMS

What devices *might* have purely random failures?

- Sensor electronics ☑
- Sensor process interfaces ☒
- Logic solver electronics ☑
- Variable speed drives ☑
- Electrical relays or contactors ☒
- Pneumatic or hydraulic devices ☒
- Actuated valves ☒

Refer to ISO/TR 12489 Annex B for explanation of random versus systematic failures

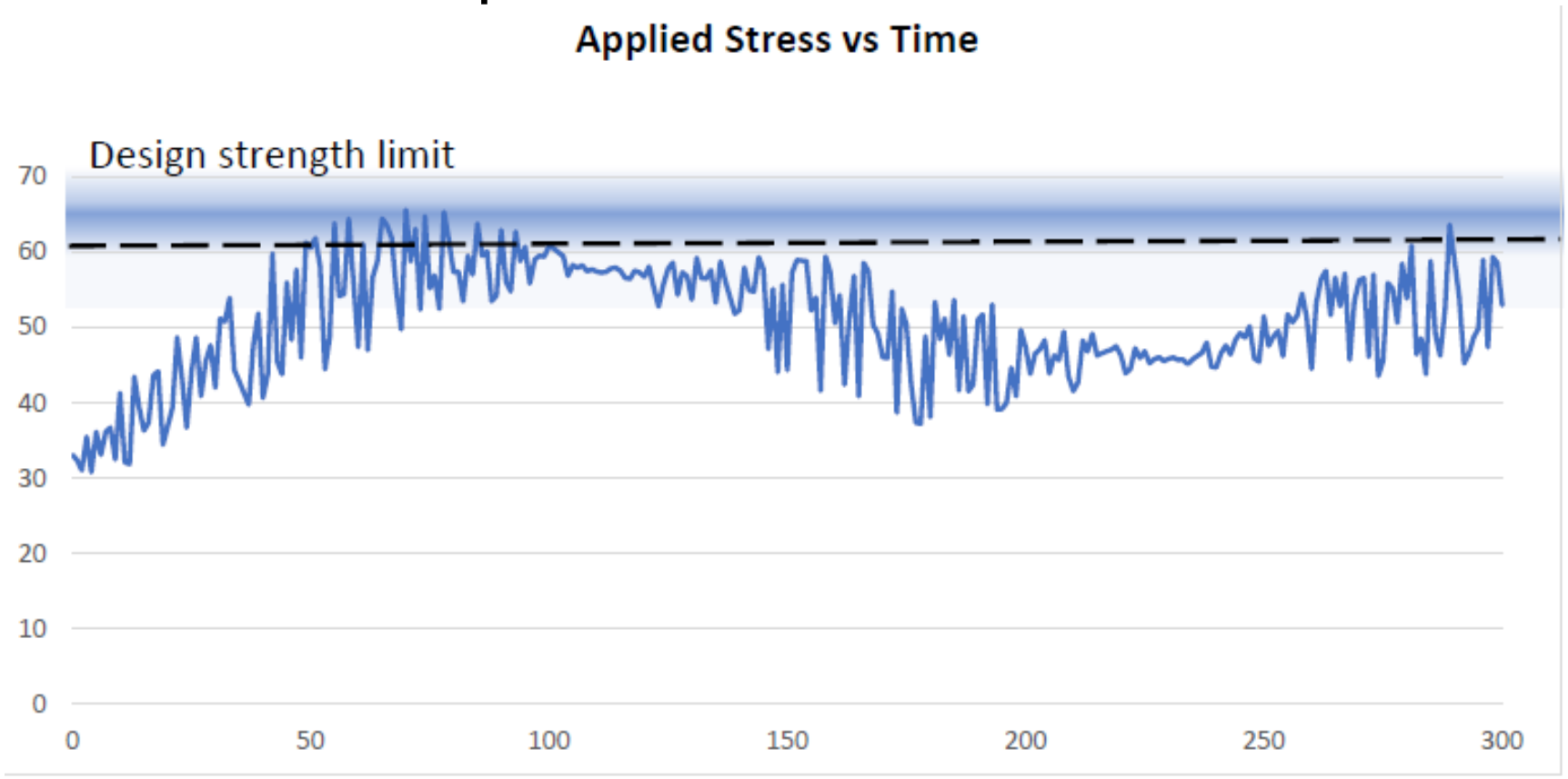
What causes purely random failure?

- Purely random behaviour is caused by a stochastic process, a series of **independent** events
- The impact of cosmic radiation on electronic components is stochastic, the rate of collisions is reasonably constant though not necessarily fixed at a single true value
- The failure rate might be reduced through radiation hardening or through fault detection and correction
- Components may be designed to withstand some damage; eventually the component failure rate might increase over time as damage accumulates, i.e. no longer purely random

SYSTEMS

Few failures are *purely* random

Most electronic component failures are **stress-related**:



After an illustration by Dr D. J. Smith in '*Reliability, Maintainability and Risk*'

Applied stress can cause *quasi*-random failure

- These failures are **dependent** on stress and strength
- Typical stress factors include:
  - Temperature
  - Shock
  - Vibration
  - Cyclic loading
  - Voltage surge
- The failure rates may **appear to be** reasonably constant, but the failures are not due to stochastic processes

SYSTEMS

All failure rates can be expected to vary

For example, refer to IEC 61709:

Electronic components – Reliability – Reference conditions for failure rates and stress models for conversion

$$\lambda = \lambda_{ref} \times \pi_U \times \pi_I \times \pi_T \times \pi_E \times \pi_S \times \pi_{ES}$$

where

λ_{ref}	is the failure rate under reference conditions;
π_U	is the voltage dependence factor;
π_I	is the current dependence factor;
π_T	is the temperature dependence factor;
π_E	is the environmental application factor;
π_S	is the switching rate dependence factor;
π_{ES}	is the electrical stress dependence factor.

SYSTEMS

Failure rates vary across orders of magnitude

- The failure rates depend on the **magnitude** and **duration** of stress, and on design strength limits
- Design strength depends on manufacturing methods, materials, tolerances, inspection, testing
- Failure rates may vary with an Arrhenius characteristic, strength degrades as damage accumulates over time
- Stress-related failure rates can be controlled by design, testing, and by reliability-centred preventive maintenance

SYSTEMS

We can always measure MTBF

…**but the failure rate does not have a fixed constant value**

Failure rate is not an ***inherent*** characteristic of any device,
it is a measure of its performance in a given environment

Confidence levels cannot be applied universally to failure rates,
but we can instead consider **uncertainty** or **variability**

SYSTEMS

Past performance reveals '**uncertainty**' interval width

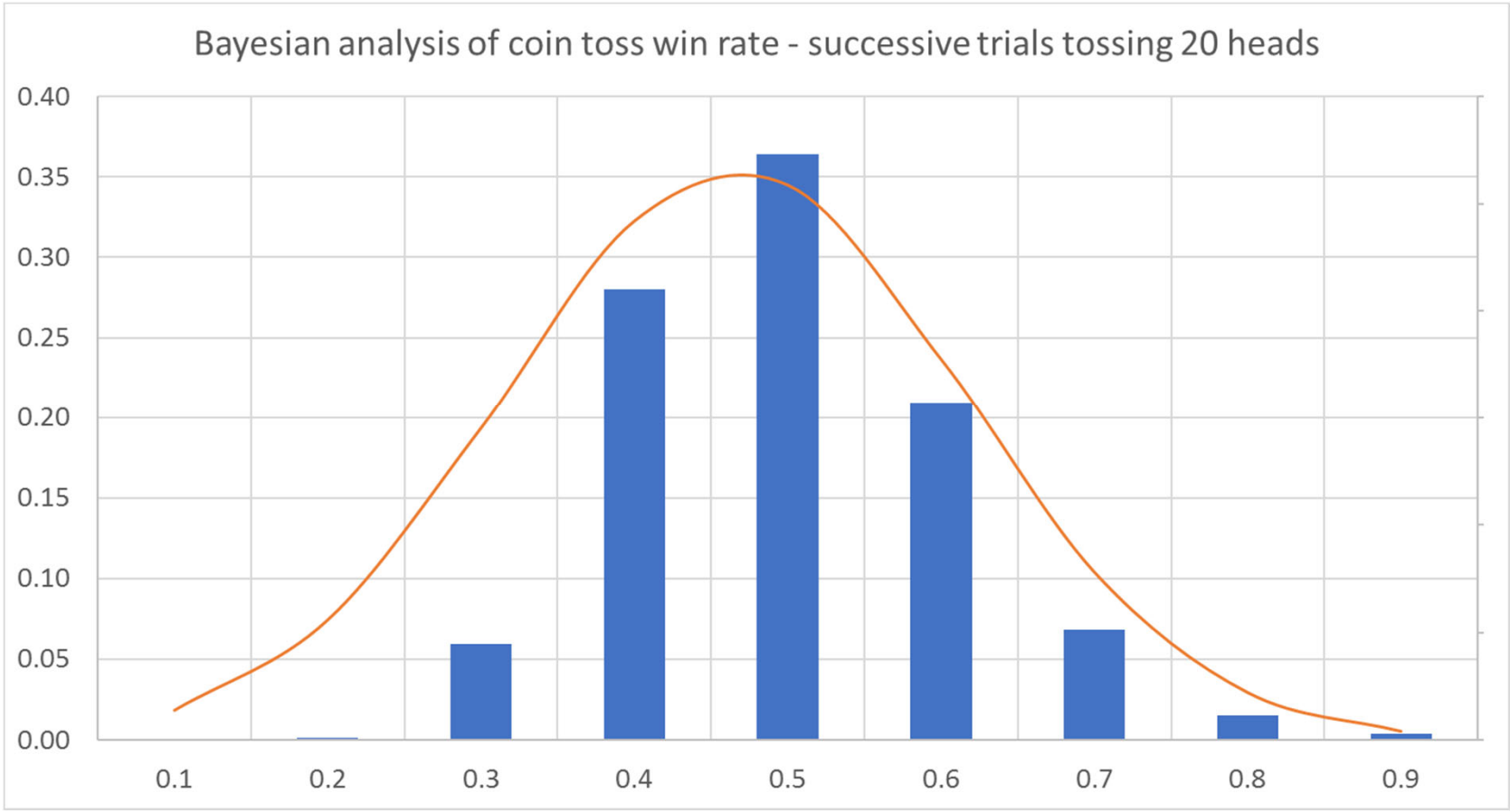
Probability distributions can always be used to model **past** performance of any system, **random or not**

We can measure time between events and use statistical techniques to estimate the mean and variance in event rates

…but that does not mean that we can precisely predict **future** performance with confidence

SYSTEMS

Is the probability of winning a coin toss constant?

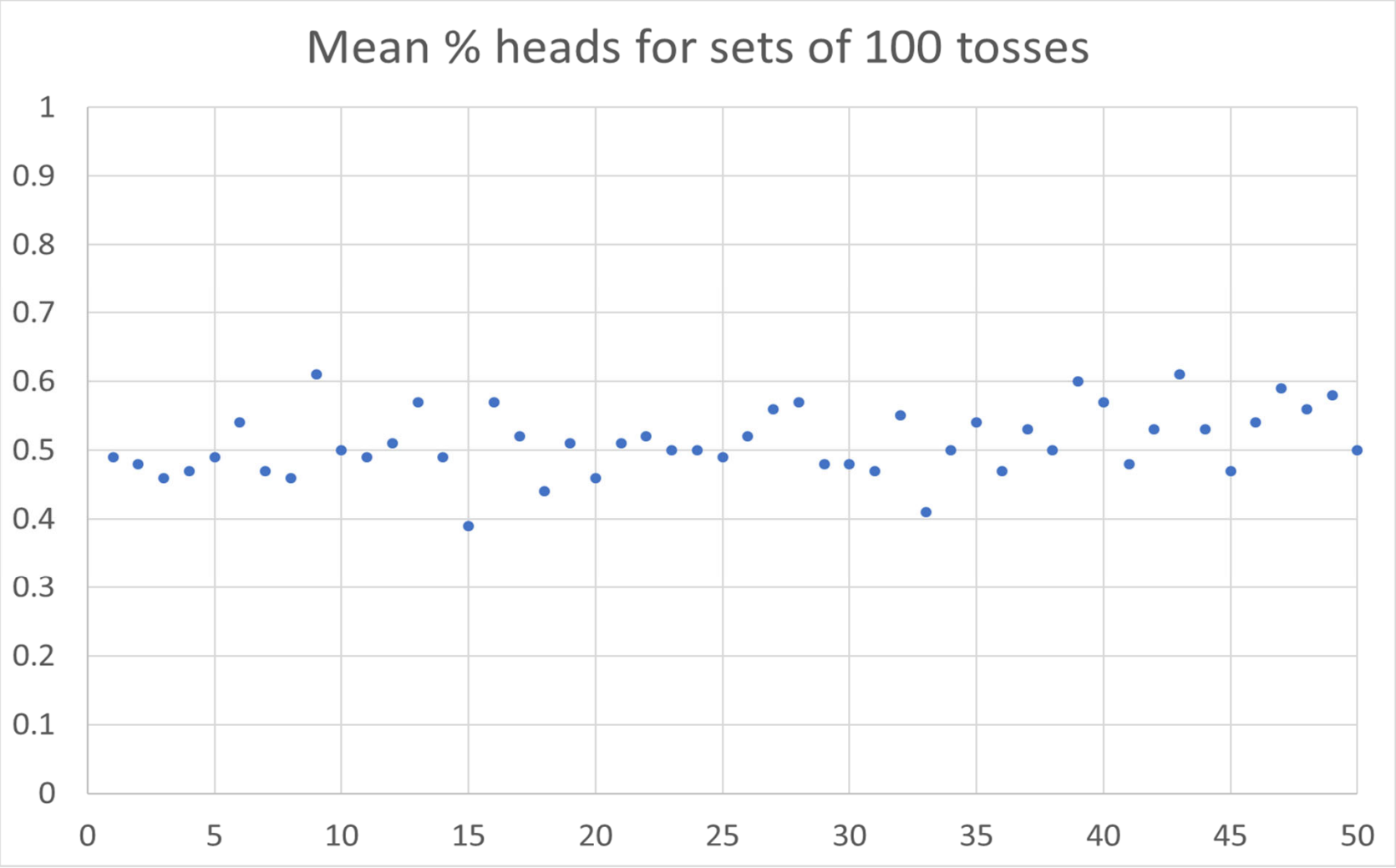


Probability distributions of coin toss trials **are constant**

- The probability of tossing ‘heads’ is **fixed**
- It is set by the balance and symmetry of the coin
- The coin has no memory
- Each toss is an independent event, purely random
- Estimated mean and variance vary slightly between trials
- The short term average varies, but…
- The long term average is fixed and constant
- Future performance can be predicted with some confidence

SYSTEMS

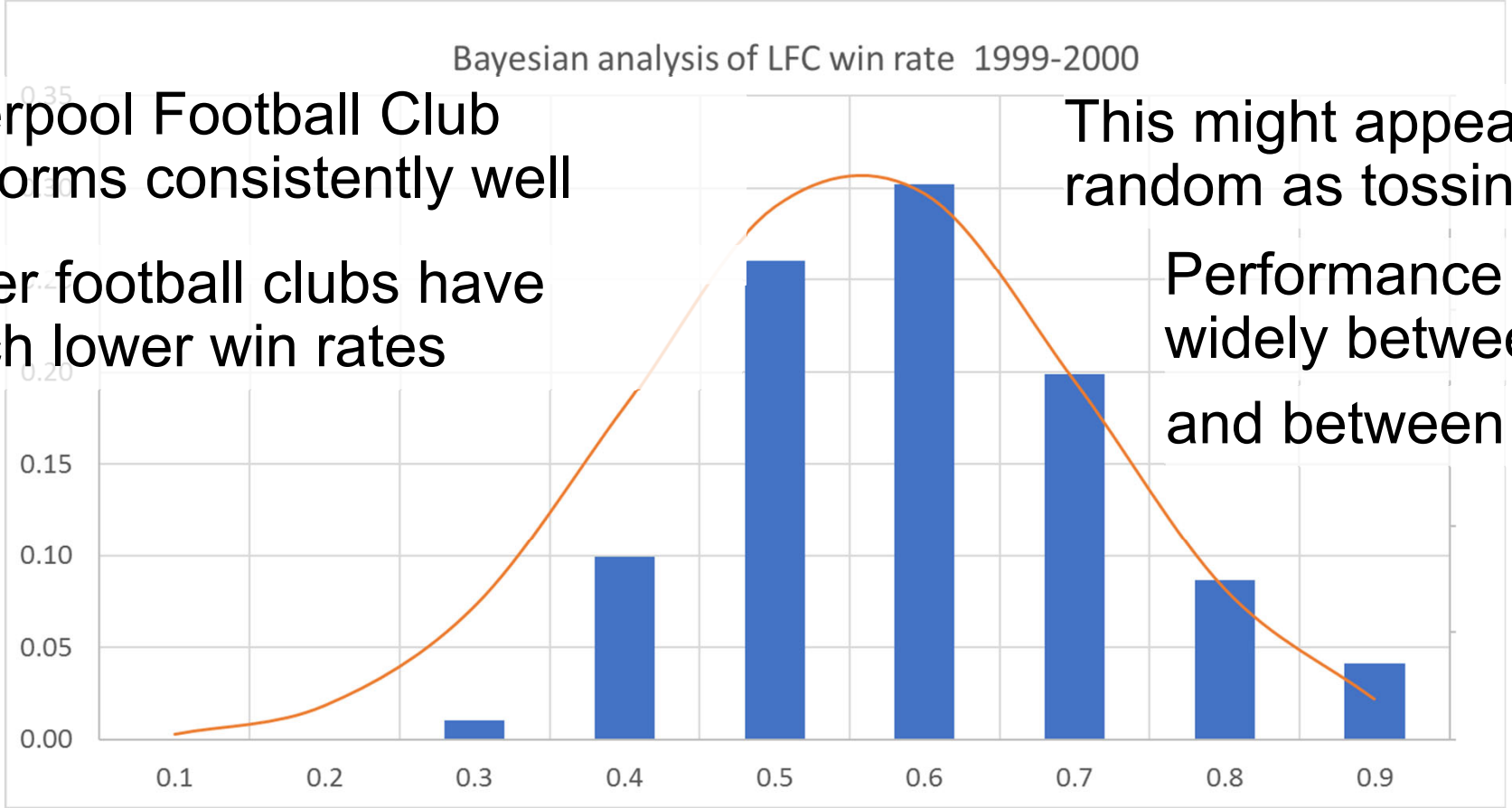
Probability distributions of coin toss trials are constant



How does football club performance vary?

Liverpool Football Club performs consistently well

Other football clubs have much lower win rates

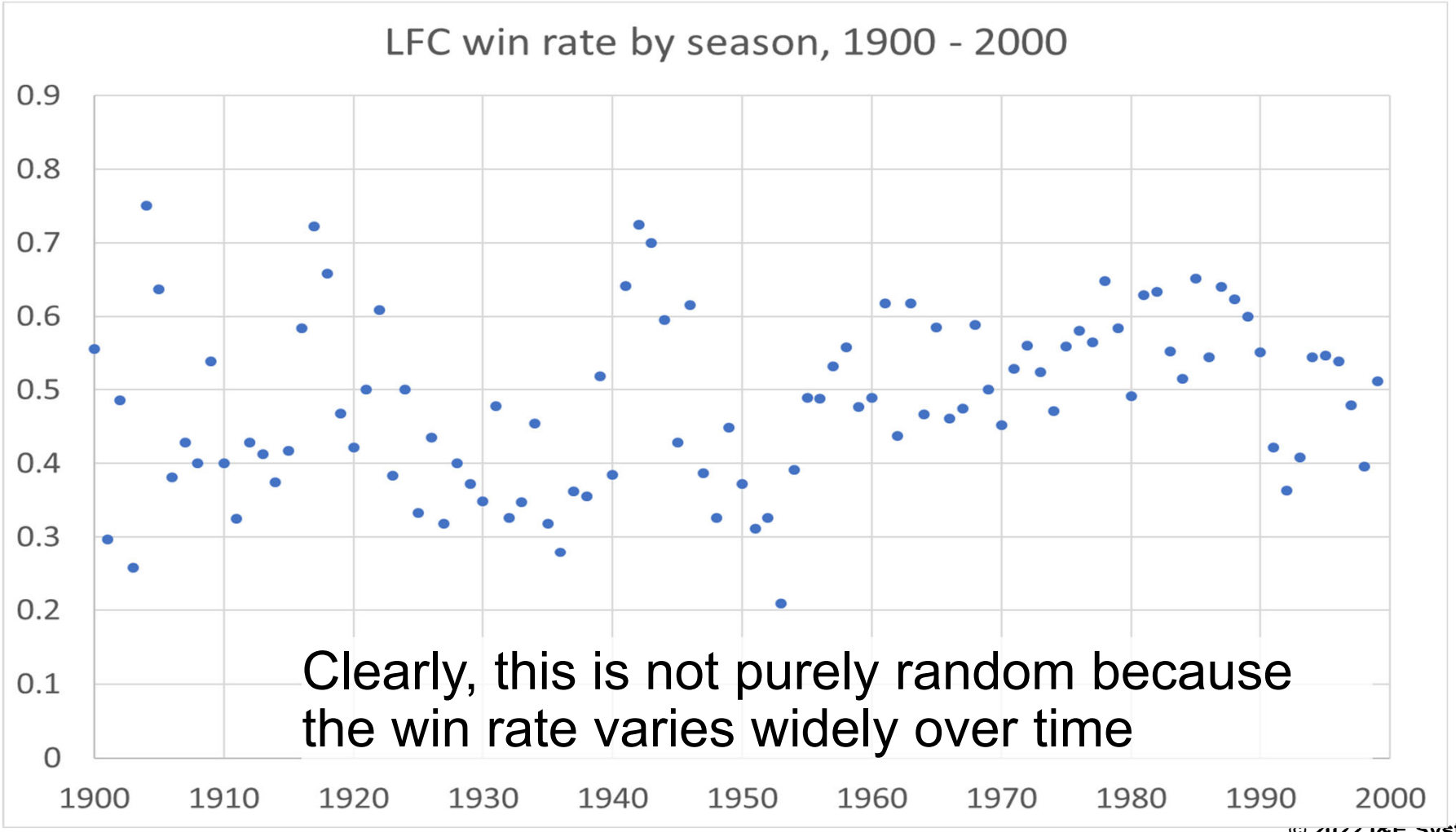


This might appear to be as random as tossing a coin

Performance varies widely between clubs

and between seasons

Football club performance varies from year to year



SYSTEMS

Football club performance varies from year to year

The probability of winning each match ***varies***,
it depends on many systematic factors

- Player ability
- Coaching techniques
- Training effectiveness
- Strategy
- Environment
- Opposition ability
- Ethical behaviour
- Good management

SYSTEMS

Safety performance also depends on team effort

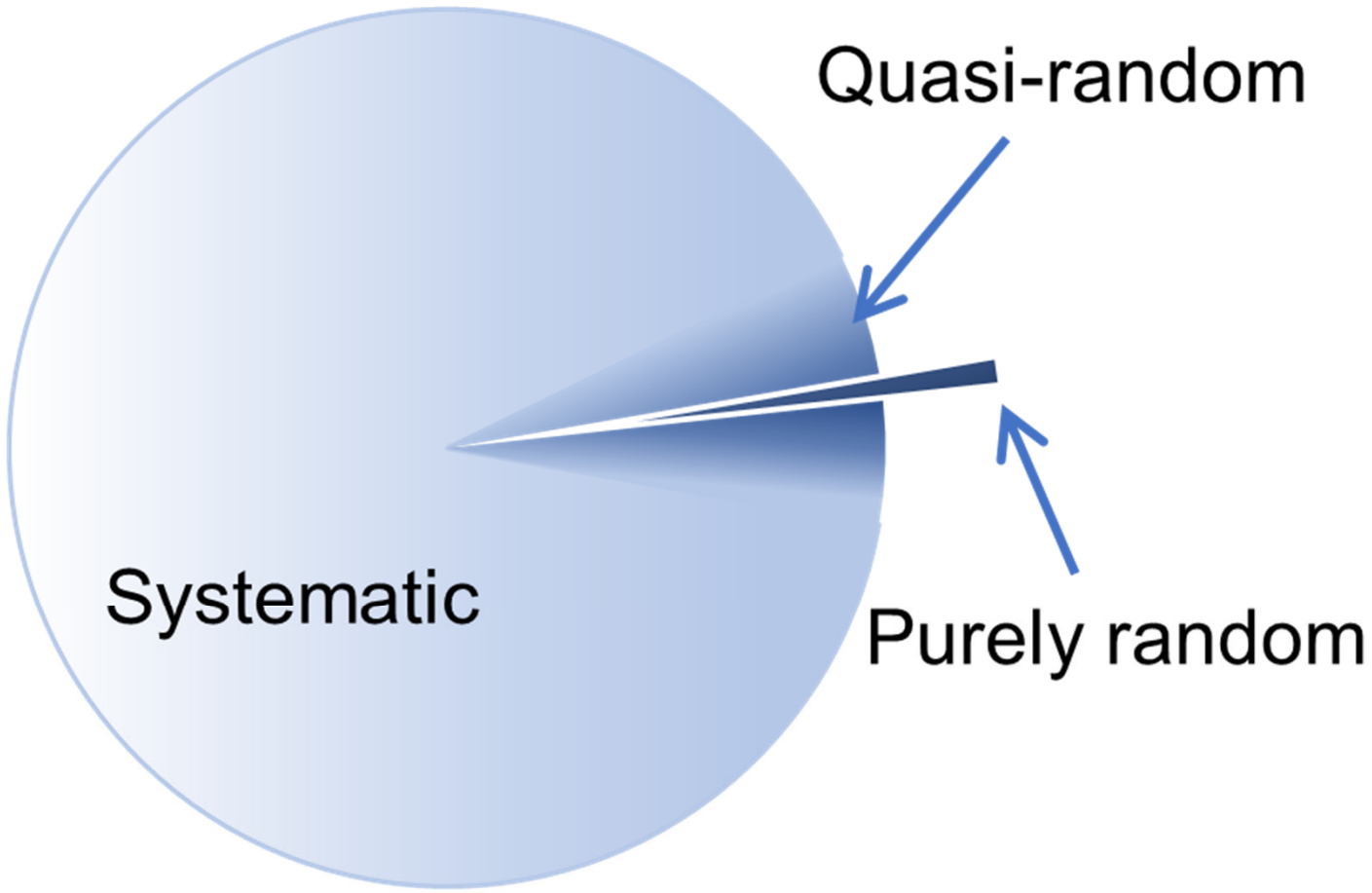
Equipment failure rates and safety incident rates depend on many influences such as

- Design quality, including suitability for service
- Installation
- Accessibility for maintenance
- Inspection and testing
- Maintenance effectiveness
- Competence
- Environment
- Good management

SYSTEMS

What proportion of safety-related failures are random?

Purely random failures are rare in industrial applications, typically < 1%



Failure rate is a performance indicator

Safety system performance is not **determined by** failure rates

Safety system performance **depends on team effort**

Failure rates are a **measure of** safety system performance

SYSTEMS

Variability in reliability data is well understood

Offshore Reliability Data – OREDA – established 1981, results first published in **1984**

The 6th edition was published in 2015

OREDA now includes onshore and offshore reliability data

Different users record different failure rates

Failure rates change over time with changing practices

The rates typically vary over **2 or 3 orders of magnitude**

OREDA summarises the mean and standard deviation as well as upper and lower deciles for equipment failure rates

SYSTEMS

Typical variation

Variation in failure rates results from differences in application, environment and maintenance effectiveness

Dr David J Smith published this summary in 2001:

Data source	90% uncertainty interval $\lambda_{95\%}$ / $\lambda_{5\%}$	Interval width, orders of magnitude
Site specific data	0.3 λ to 3.5 λ	1.1
Industry specific data	0.2 λ to 5 λ	1.4
Generic data	0.1 λ to 8 λ	1.8

Smith, D. J. *'Reliability, Maintainability and Risk'*, 6th Ed. Butterworth Heinemann. 2001

SYSTEMS

Failure rates can be estimated at a ‘certainty’ level

Failure rates that are achieved by at least 70% of users can be estimated using readily available sources such as:

- OREDA
- *exida* Safety Equipment Reliability Handbook
- FARADIP

Failure rates at around the 90% or 95% certainty level are typically a **factor of 3** higher than the 70% level

SYSTEMS

Maintenance effectiveness

From Bukowski, J.V. and Stewart, L. :

'*Quantifying the Impacts of Human Factors on Functional Safety*'

American Institute of Chemical Engineers' 12th Global Congress on Process Safety, Houston, Texas. 2016

Ineffective maintenance results in probability of failure
3 or 4 times higher than 'normal' maintenance practices

OREDA datasets are consistent with a similar conclusion:

$$\lambda_{95\%} \approx 3 \times \lambda_{70\%}$$

SYSTEMS

Conclusions

With site-specific data, we can expect that a 90% uncertainty interval spans ***at least*** one order of magnitude

Worst case performance may be more than 3 times worse than 'normal'

Best practice performance could be at least 3 times better than normal and maybe as much as 10 times better

SYSTEMS

Achieving best practice

Failure performance depends on deliberate decisions and strategies applied to prevent preventable failures

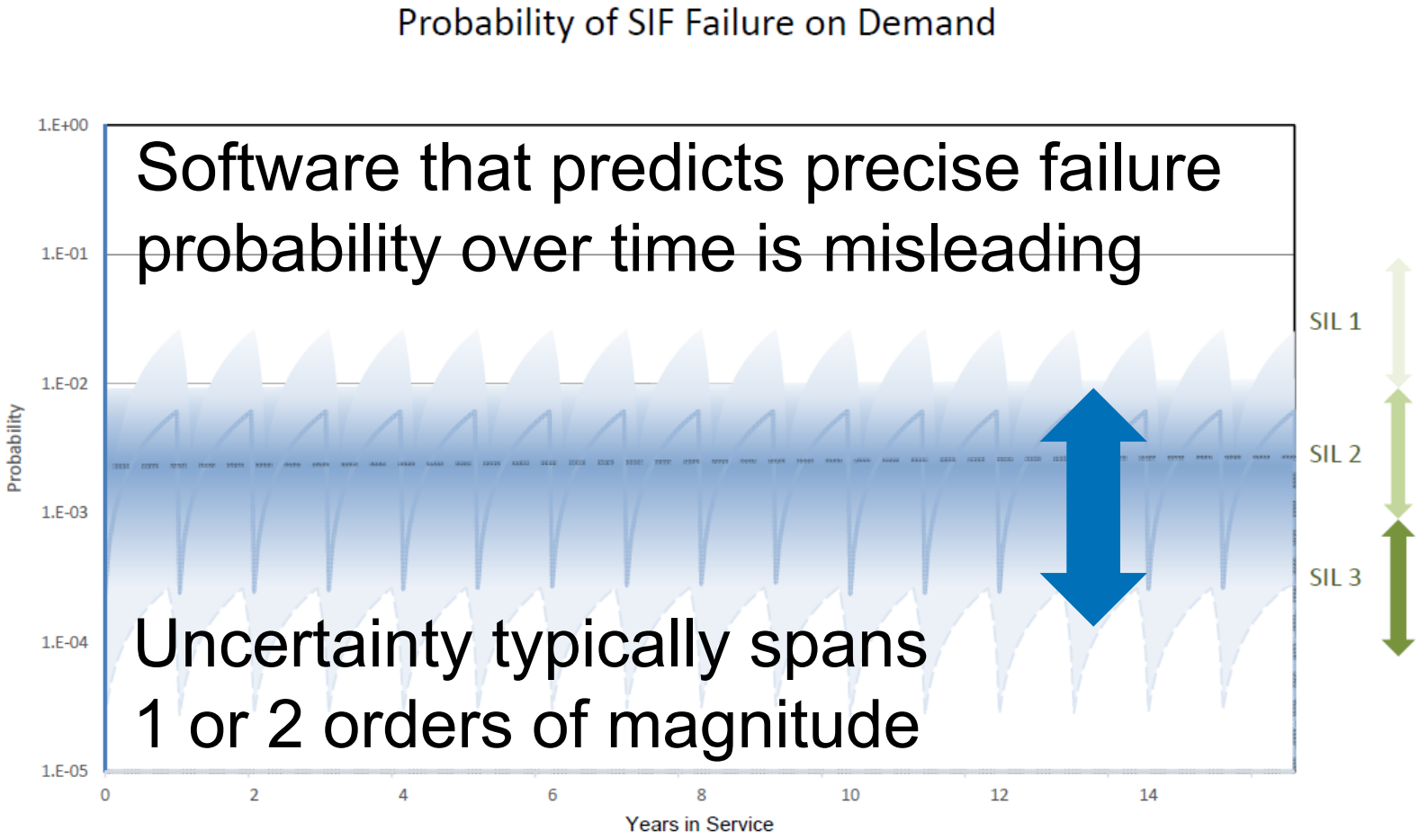
Best practice performance can be achieved **at a cost** with **reliability centred maintenance**

(e.g. aviation industry, defence industry)

Failure performance cannot be predicted with certainty because it depends on human behaviour

SYSTEMS

Failure probability estimates can never be precise



SYSTEMS

Back to our objective

'reliability data uncertainties shall be assessed and taken into account when calculating the failure measure'

A result such as $RRF_{AVG} \approx 317$
could be expressed more realistically as:

$RRF_{AVG} \approx$ 300 if the maintenance is as effective as planned

though RRF_{AVG} may be < 100 if maintenance is not effective

SYSTEMS

Should this level of uncertainty be acceptable?

Yes, of course, because risk and risk reduction targets can only be estimated to within half an order of magnitude at best

Uncertainty with a factor of > 3 is normal in risk assessment

It is important for users to understand that risk reduction achieved by safety functions is **dependent** on decisions made in design, operation and maintenance

SYSTEMS

Questions?

Recommended reading:

Moubray, J. '*Reliability-centred Maintenance*'

Smith, D. J. '*Reliability, Maintainability and Risk*'

SYSTEMS