# 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

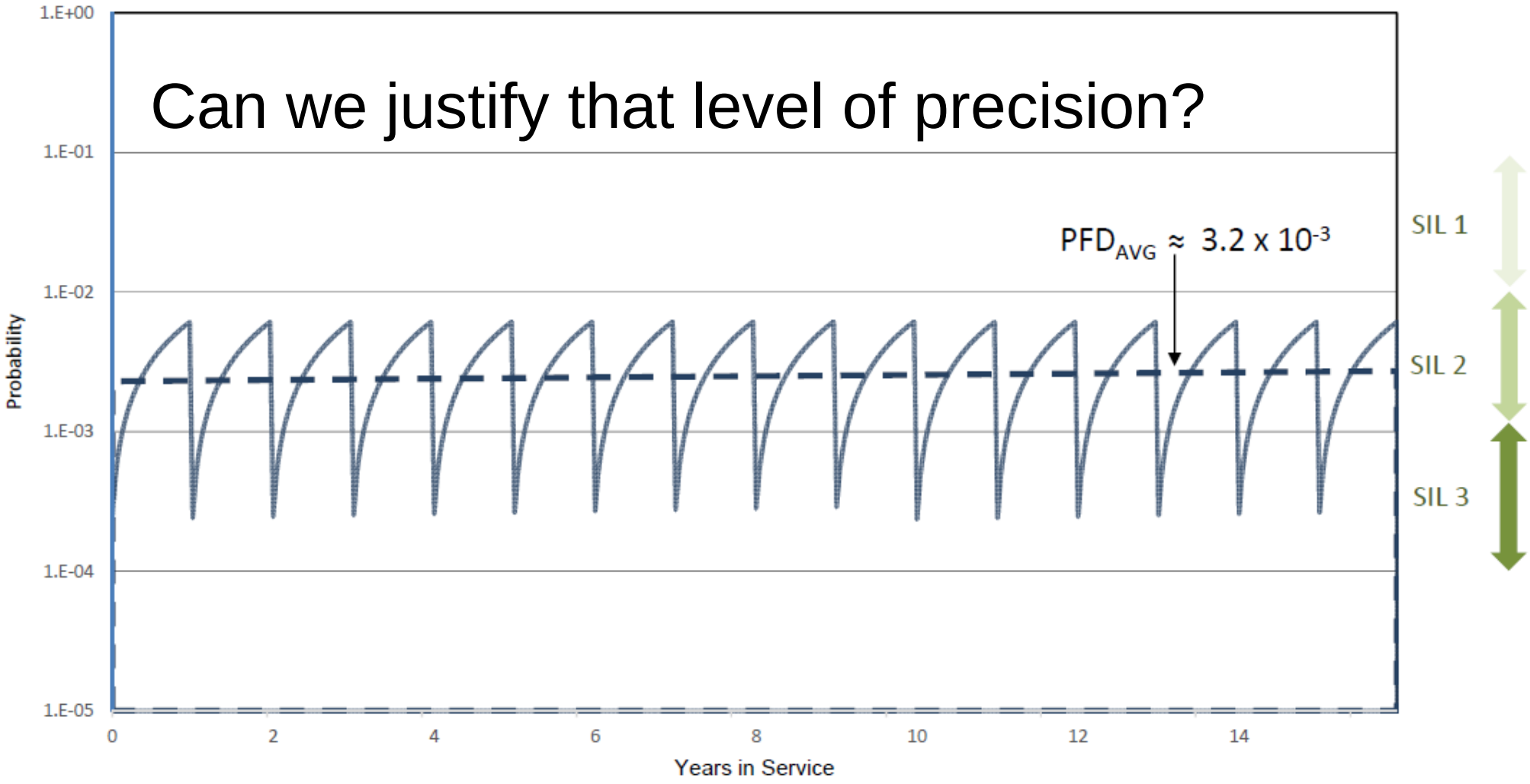
Calculation results are presented confidently with precision:

$PFD_{AVG} \approx 0.00315$ and $RRF \approx 317$

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**

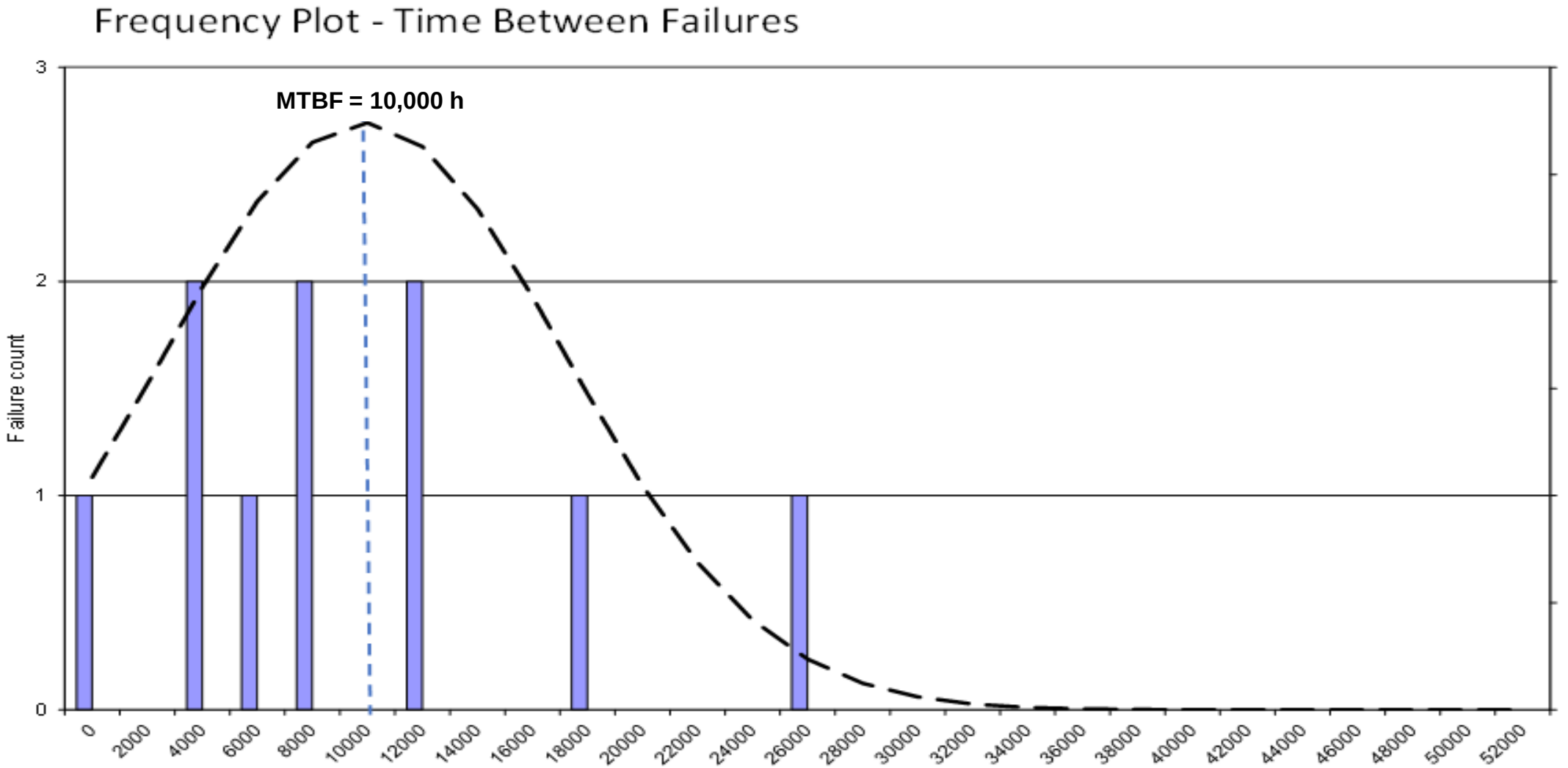
***If*** a failure rate is reasonably constant, the failure rate can be estimated from the **mean time between failures**:

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

Occurrence of random failures follows a Poisson distribution because each failure is a **purely independent event**

SYSTEMS

# Time between failures follows a normal distribution



# Time between failures follows a normal distribution

Because of the Poisson distribution, the time between failures will follow a normal distribution around the MTBF

If that assumption is valid we can use a **chi-square function** to estimate the true MTBF and failure rate - even if only a few failures have been recorded

SYSTEMS

# Confidence levels from chi-square

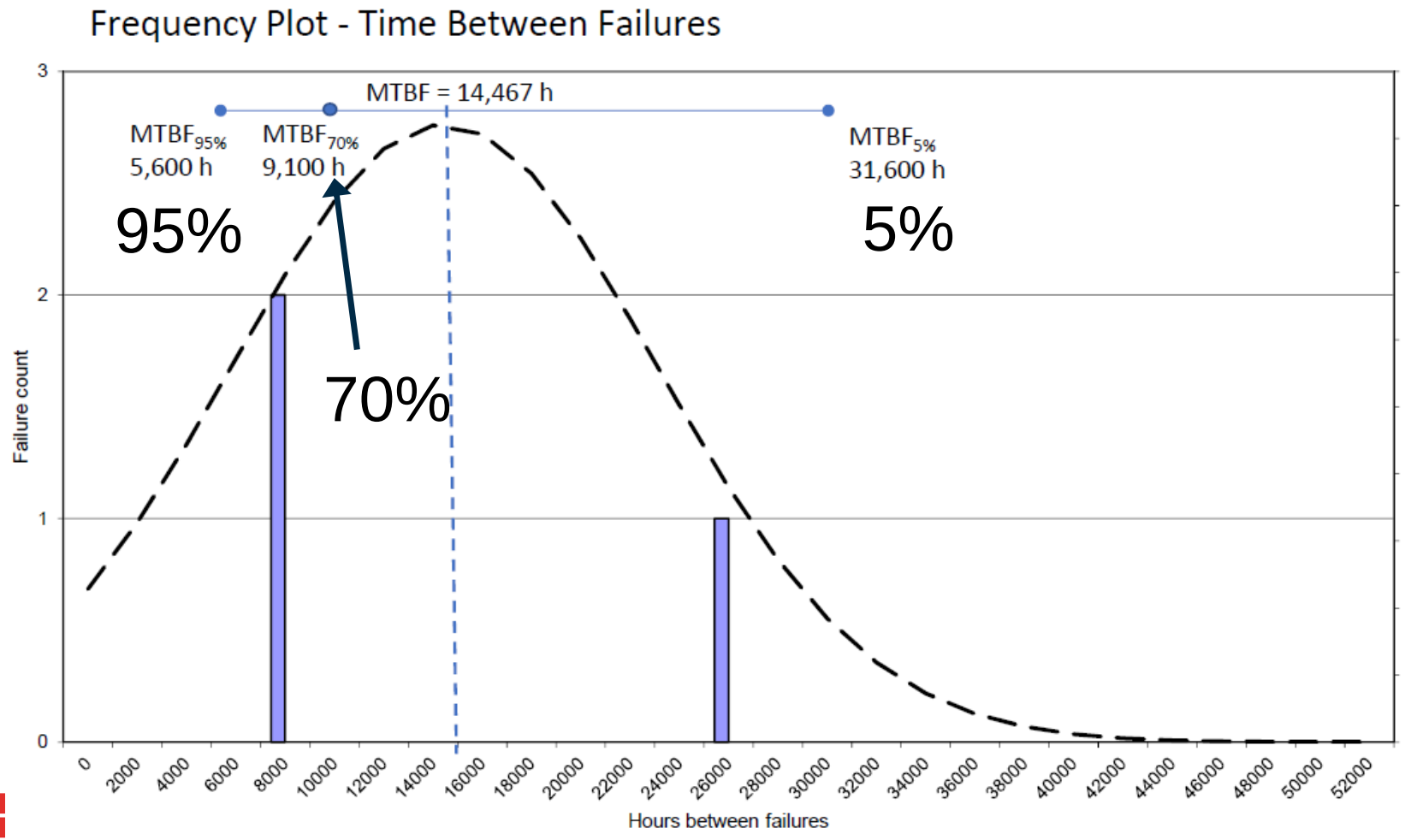
The chi-square function is based on the normal distribution

It enables estimates to be made at any desired level of confidence with any number of failures

- The estimate $MTBF_{70\%}$ is at the 70% **confidence level**: there is a 30% chance that the true long term MTBF will be worse (lower) than $MTBF_{70\%}$
- We can define a **confidence interval**:
  There is a 90% chance that the true long term MTBF will be between $MTBF_{5\%}$ and $MTBF_{95\%}$

SYSTEMS

# MTBF can be estimated with only a few failures




SYSTEMS

# MTBF can be estimated from any number of failures

The chi-square function uses

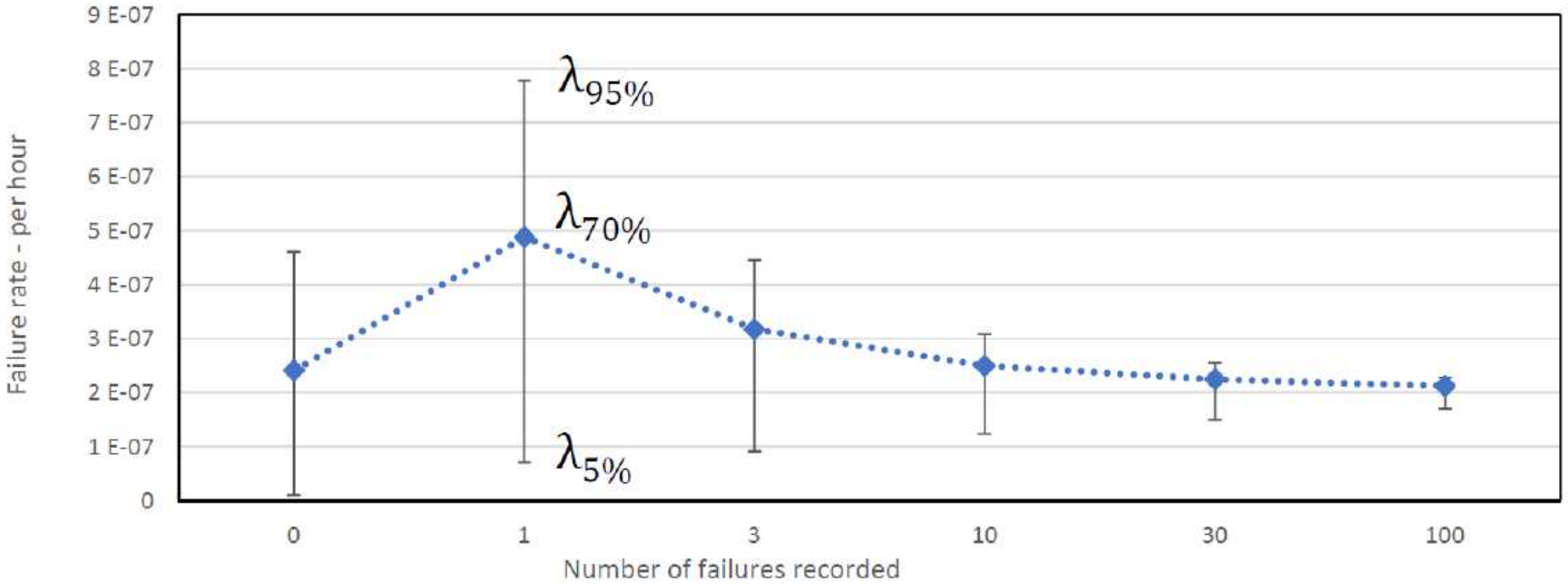
- Total time in service (device-hours)
- Number of failures

The confidence level is based on the mean and standard deviation of a normal distribution

MTBF can even be estimated with **zero** failures, based on total time in service

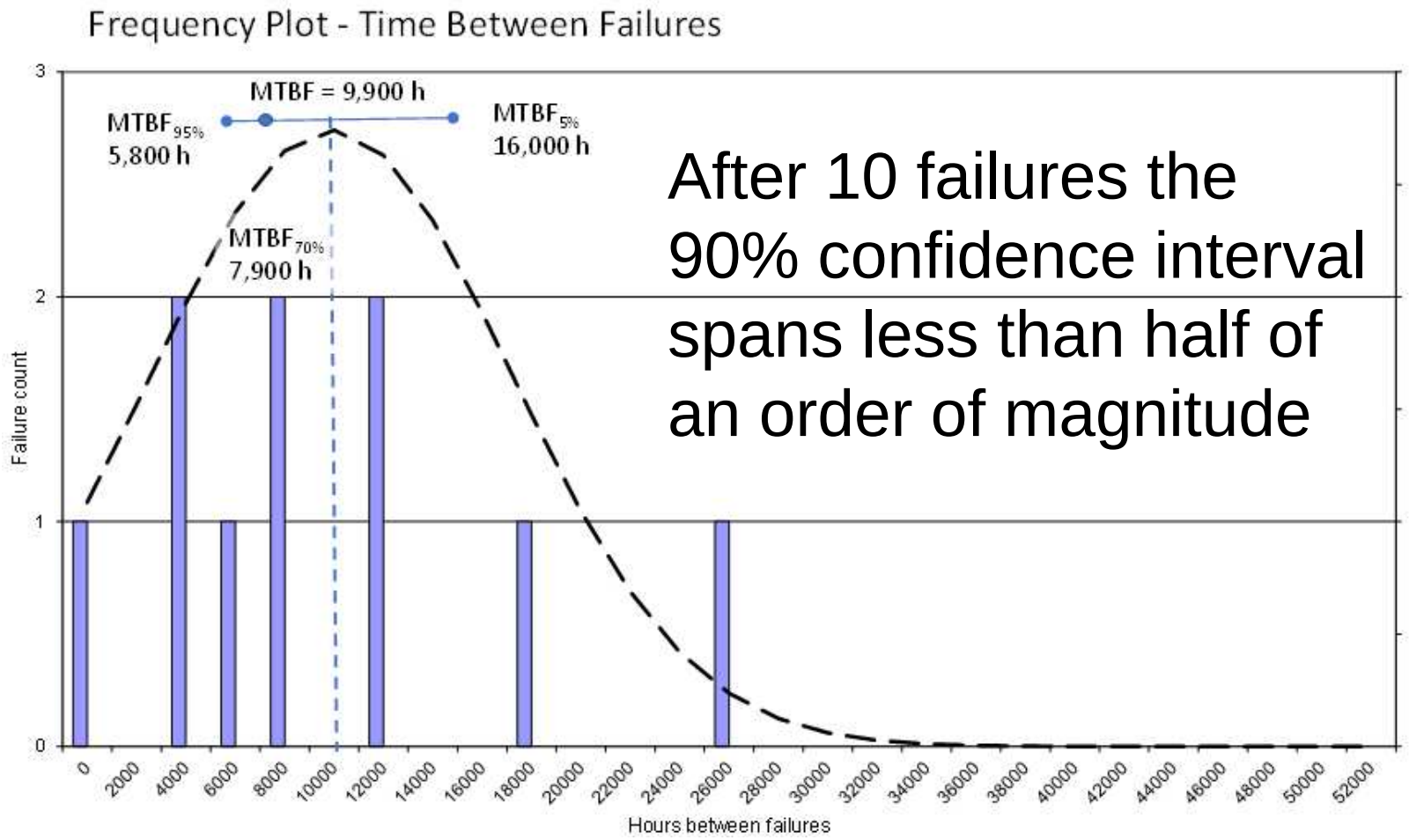
SYSTEMS

# Confidence interval width reduces with failure count




SYSTEMS

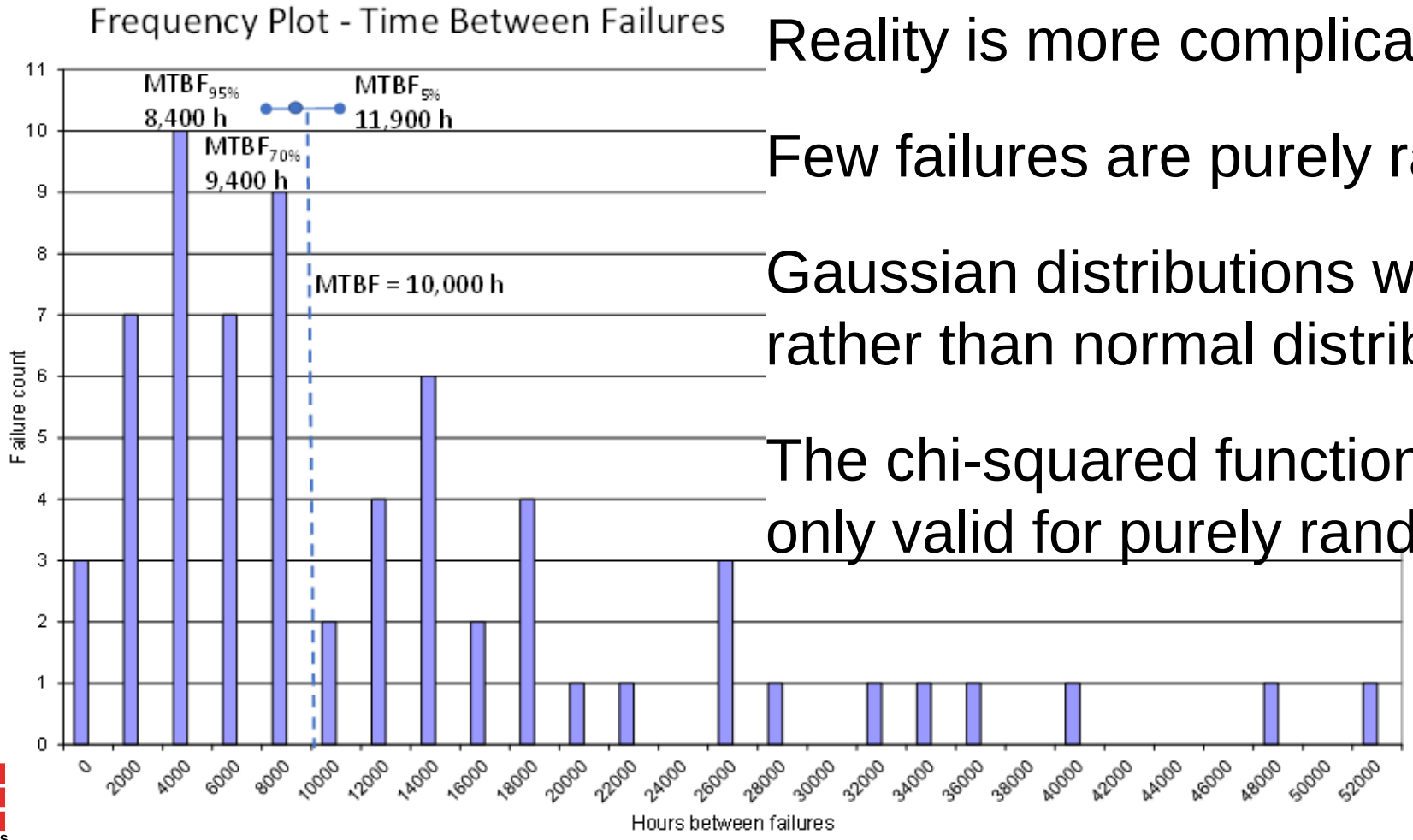
# Confidence interval width reduces with failure count




After 10 failures the 90% confidence interval spans less than half of an order of magnitude

SYSTEMS

# But this theory does not always work in practice




Reality is more complicated

Few failures are purely random

Gaussian distributions would apply rather than normal distributions

The chi-squared function is only valid for purely random failure

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 ☒

SYSTEMS

# The cause of purely random failure

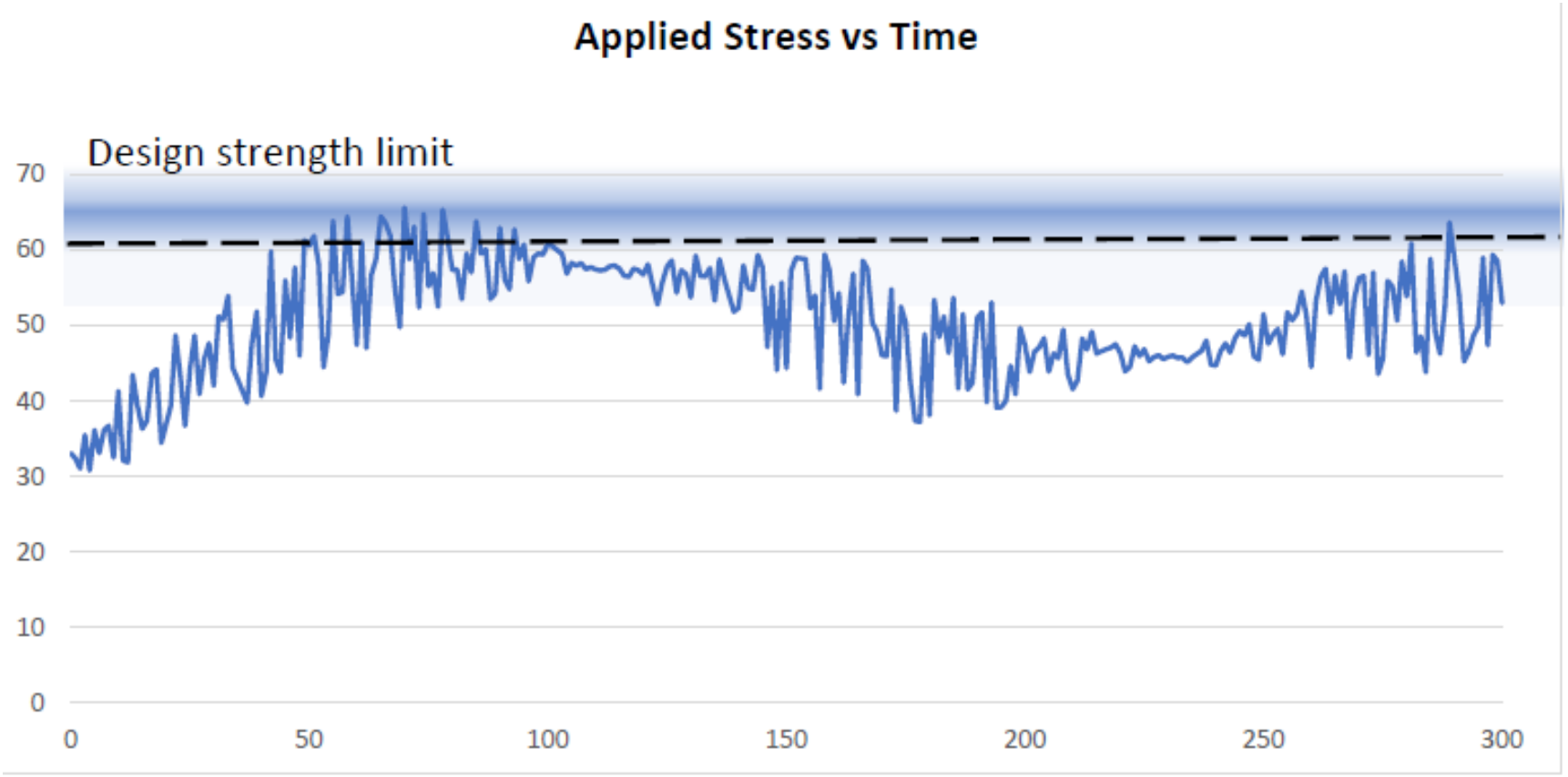
- Purely random behaviour is caused by a stochastic process, a series of **independent** events
- The impact of cosmic radiation on electronic components is stochastic, the rate of collisions is reasonably constant
- The failure rate might be reduced through radiation hardening or through fault detection 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:

(based on an illustration in Smith, D. J. '*Reliability, Maintainability and Risk*')




SYSTEMS

# Applied stress can cause *quasi*-random failure

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

# Quasi-random failure rates vary widely

- The failure rate depends on the **magnitude** and **duration** of the stress, and on the design strength limit
- Design strength depends on manufacturing methods, materials, tolerances, inspection, testing
- The failure rate 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 there is no underlying constant failure rate**

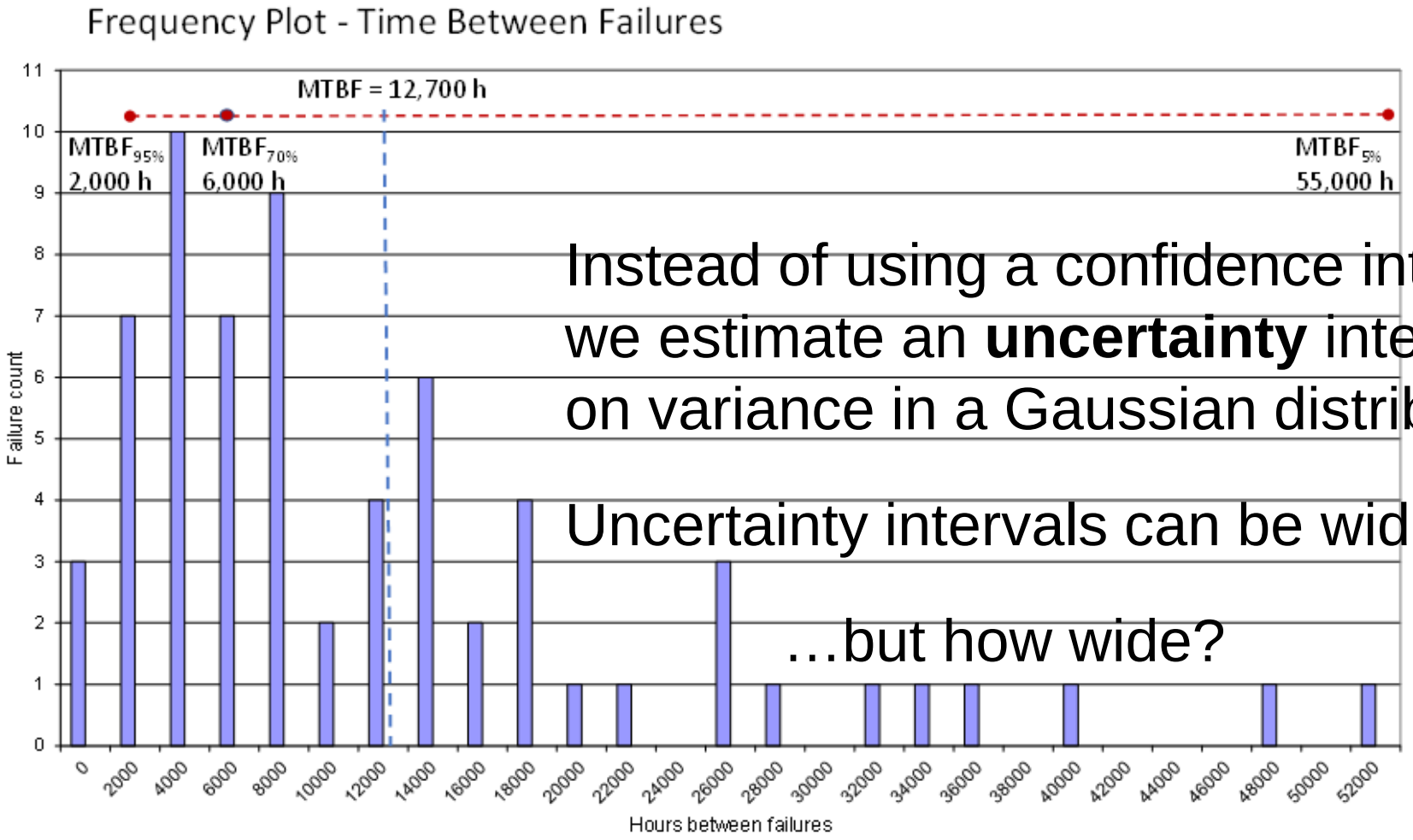
$$\lambda \neq 1/\ \mathrm{MTBF}$$

A failure rate $\lambda$ can always be measured, but it varies
Failure rate is not an ***inherent*** characteristic of any device,
it is a measure of device performance in a given environment

Confidence levels are meaningless and cannot be applied,
but we can instead consider **uncertainty** or **variability**

SYSTEMS

# Reality is uncertain




Instead of using a confidence interval we estimate an **uncertainty** interval based on variance in a Gaussian distribution

Uncertainty intervals can be wide

…but how wide?

SYSTEMS

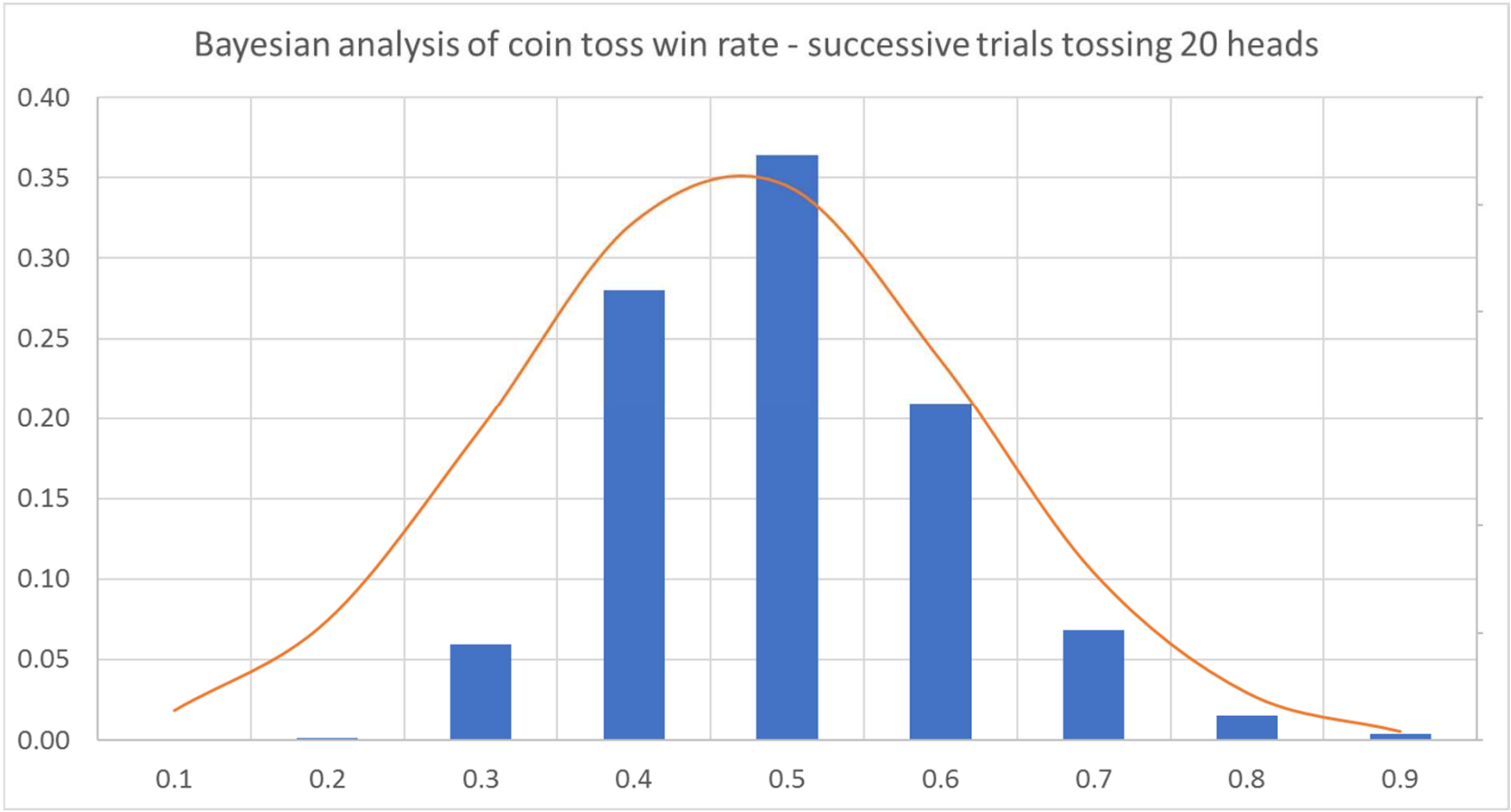
# Past performance reveals uncertainty interval width

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

SYSTEMS

# Is the probability tossing a head constant?

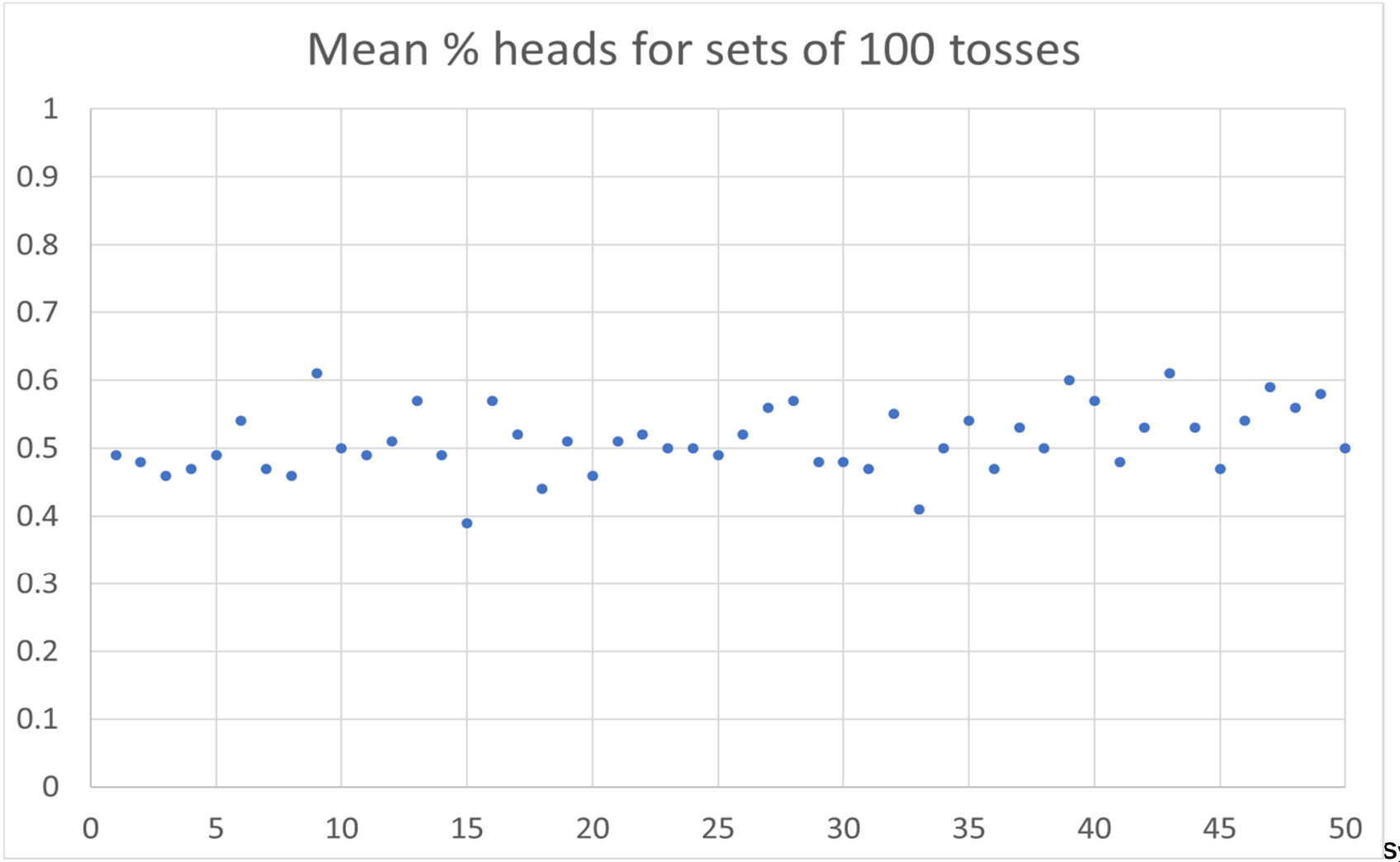


# Probability distributions of coin toss trials are constant

- The probability of tossing a head 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



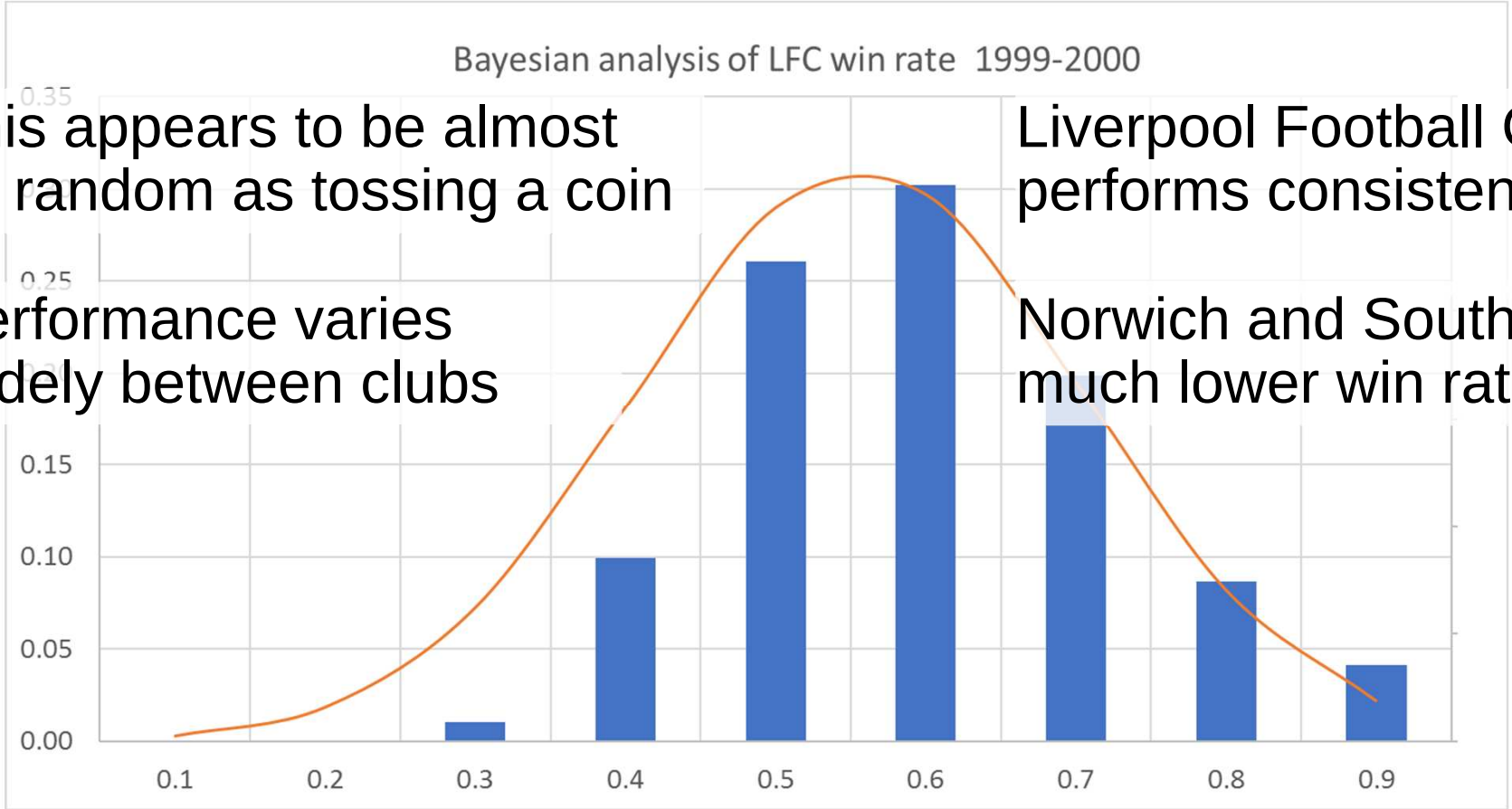
# How does football club performance vary?

This appears to be almost as random as tossing a coin

Performance varies widely between clubs

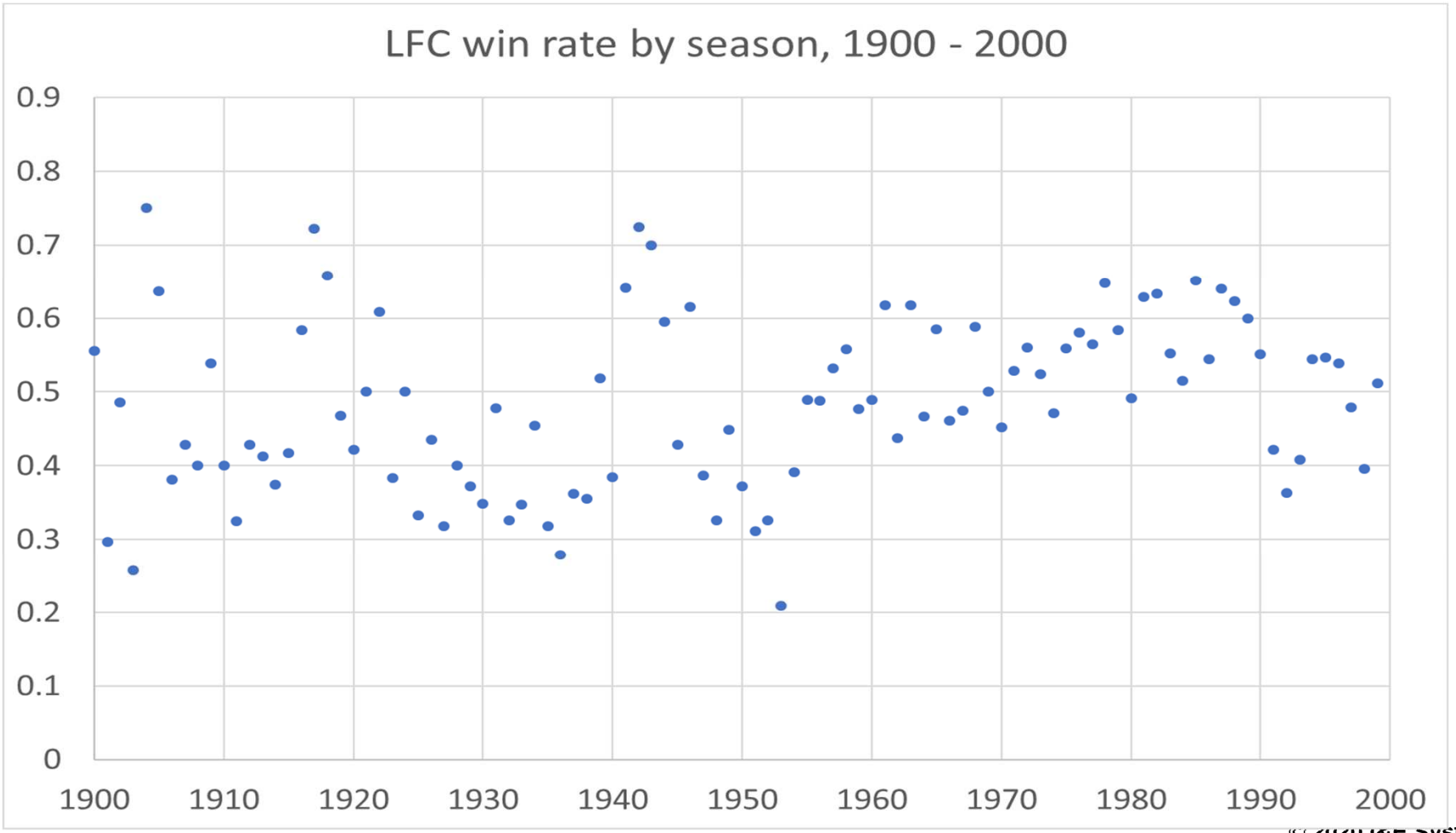
Liverpool Football Club performs consistently

Norwich and Southend have much lower win rates




SYSTEMS

# 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

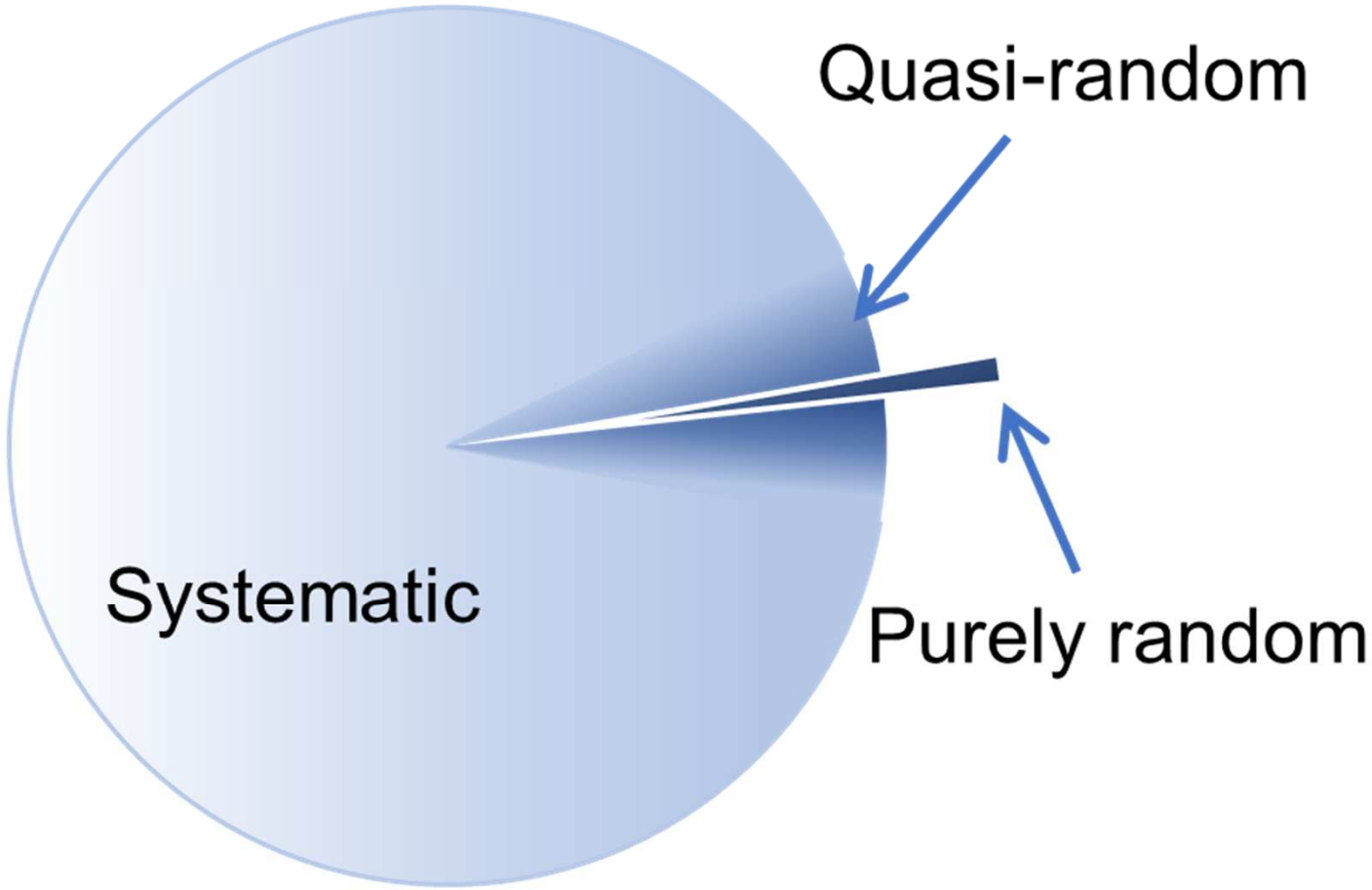
Equipment failure rates and safety incident rates depend on many influences such as

- 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




SYSTEMS

# Failure rate is a performance indicator

Safety system performance is not determined by failure rates

Failure rates are a measure of safety system performance

Safety system performance **depends on team effort**

Past performance is no guarantee of future performance; performance can be changed through deliberate action

SYSTEMS

# Variability in reliability data is well understood

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

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

Dr David 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 any 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 the 90% or 95% certainty level are typically higher than the 70% level by a **factor of 3**

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 up to **4 times higher** than 'normal' maintenance practices (achieved by 70% of users)

OREDA datasets are consistent with a similar conclusion:

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

$$MTBF_{95\%} \approx 0.3 \times MTBF_{70\%}$$

SYSTEMS

# Conclusions

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

As a rough approximation, we can simply assume:

$\lambda_{95\%} \approx 3\ \lambda_{70\%}$ $\quad$ $MTBF_{95\%} \approx 0.3\ MTBF_{70\%}$

$\lambda_{5\%} \approx 0.3\ \lambda_{70\%}$ $\quad$ $MTBF_{5\%} \approx 3\ MTBF_{70\%}$

**The worst case performance is 3 times worse than normal**

The best case performance could be at least 3 times better

SYSTEMS

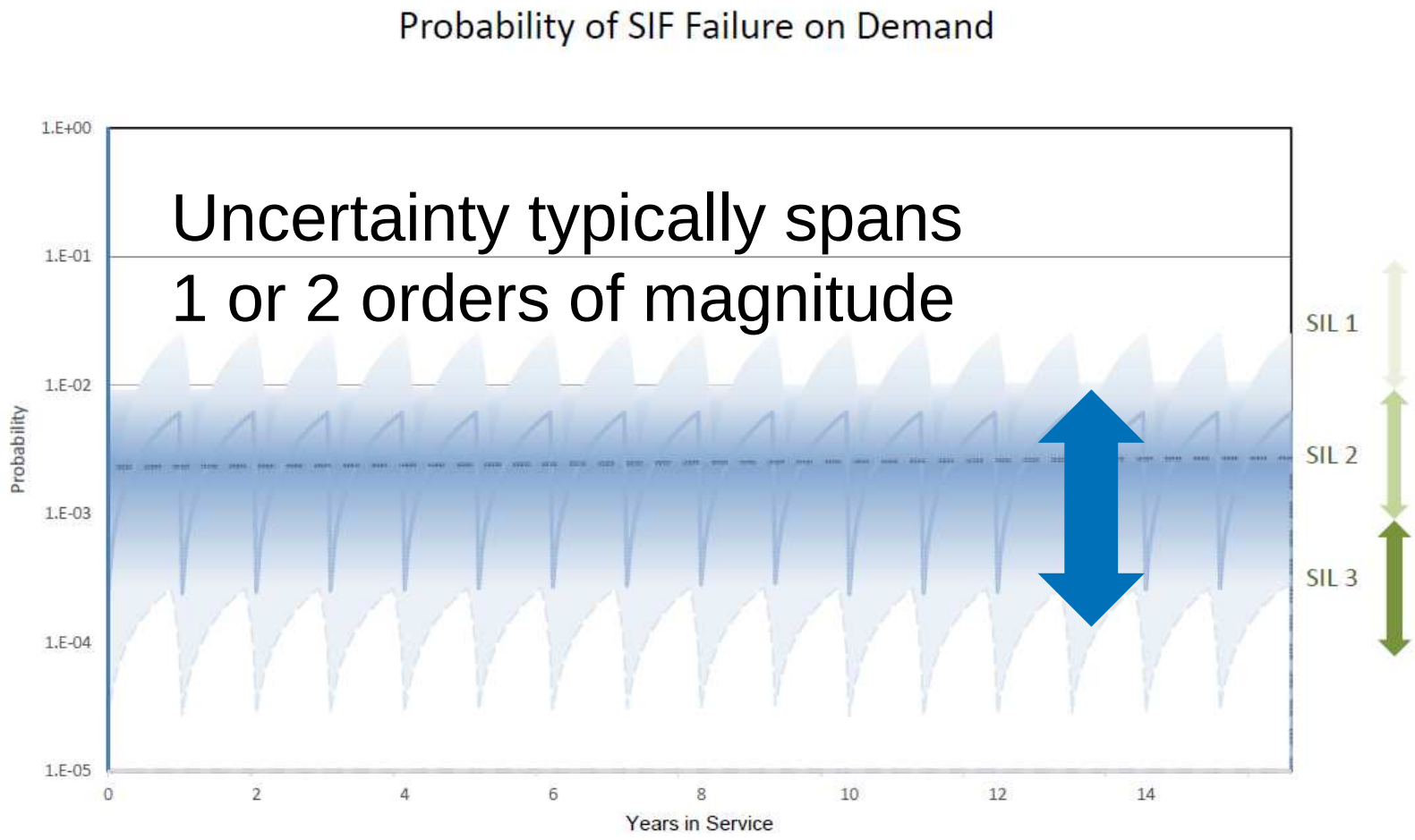
# Achieving best practice

Best practice performance can be achieved **at a cost** with **Reliability Centred Maintenance**

(e.g. aviation industry, defence industry)

SYSTEMS

# Failure probability estimates can never be precise




SYSTEMS

# The best possible case – electronic safety functions

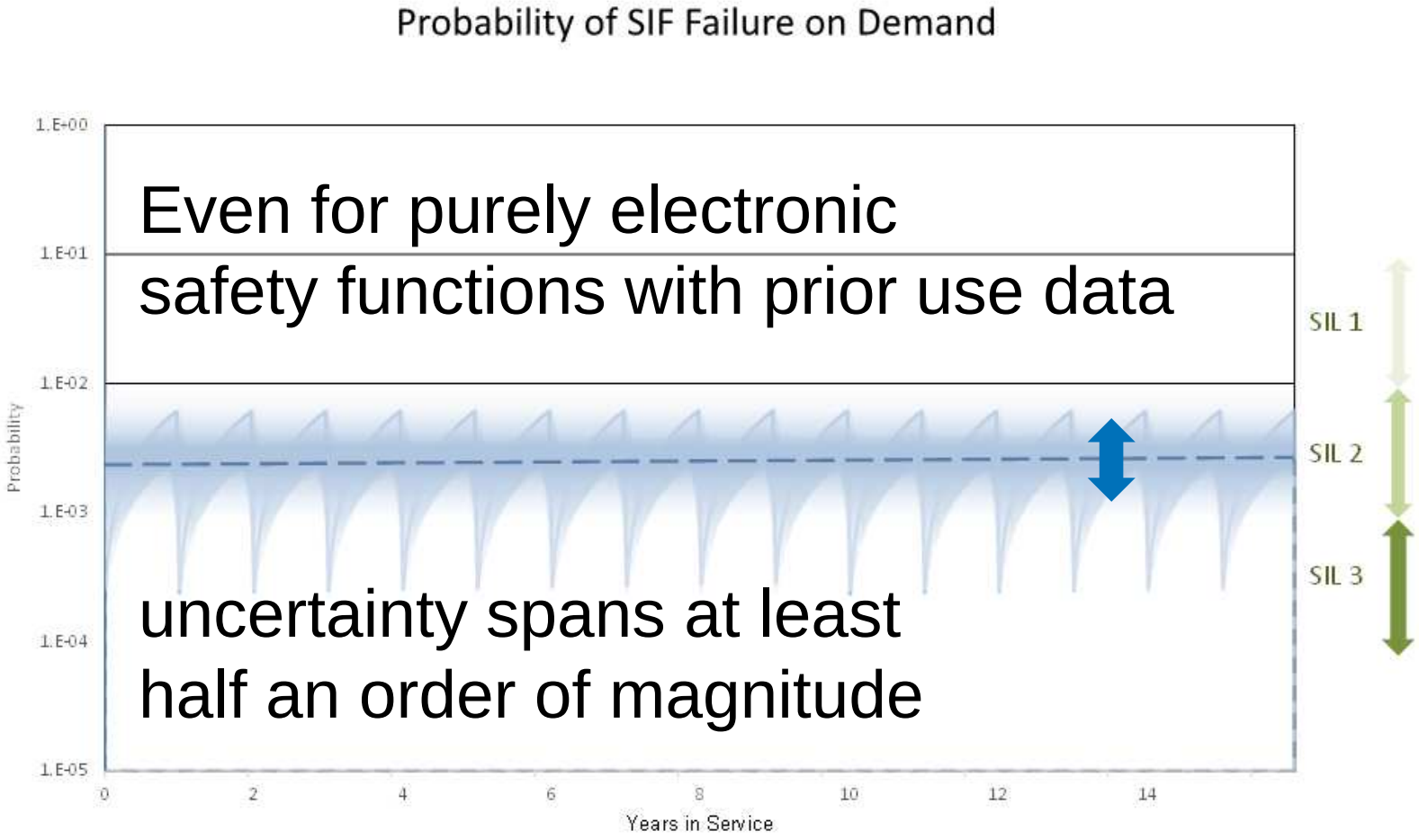
Even with purely electronic safety functions and **prior-use**,

the uncertainty interval width is always at least
**half an order of magnitude**

(i.e. a factor of 3 from top to bottom)

SYSTEMS

# Minimum plausible uncertainty interval width




SYSTEMS

# So back to our objective

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

A result such as $RRF_{AVG} \approx 317$ $(PFD_{AVG} \approx 0.00315)$ could be expressed more realistically as:

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

***but*** there is a 30% chance that the RRF will be lower and $RRF_{AVG} \approx 100$ can be expected with worst case performance

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

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