
# What does functional safety mean?

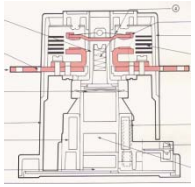
# What is functional safety?

- **It is about things working safely and productively**
- It is about a methodology for a safe design
- **It is about** how to demonstrate it is safe
- **It is about implementing a** solution that takes into account **technical and economic aspects**

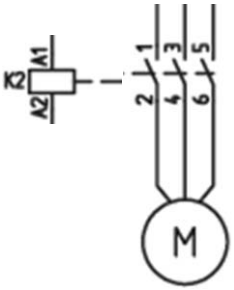

CAPIEL
european coordinating committee of manufacturers of electrical switchgear and controlgear

# What makes safety specific

- **Is a contactor controlling a motor  driving a fan a safety device**



?




CAPIEL
european coordinating committee of manufacturers of electrical switchgear and controlgear

# Contactor in its intended application

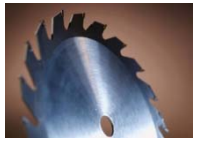
- **What happens if the contactor doesn't work?**
- **How does it fail?**
- **Does the contactor fail in the on/off/unknown state?**
- **Do any of these states represent a dangerous state?**
- **In this case of building ventilation, most of the failures are inconvenient rather than dangerous**

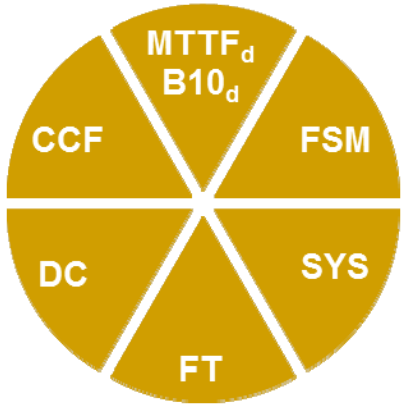
CAPIEL
european coordinating committee of manufacturers of electrical switchgear and controlgear

# Contactor in machine application

- **There is a risk – how high is the risk (occurrence, severity)?**
- **Is a normal contactor good enough?**
- **How do we know?**
- **What do we need to do to check that it is good enough?**

**We need to apply a functional safety methodology**



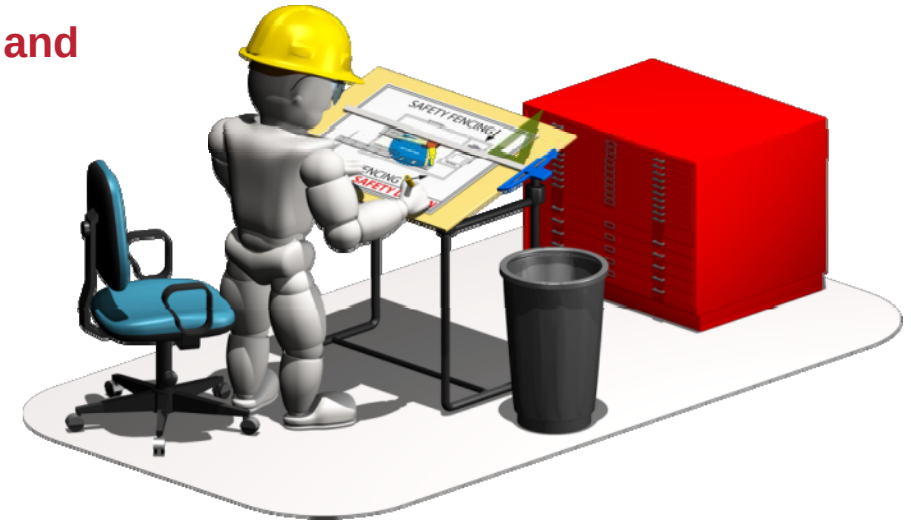


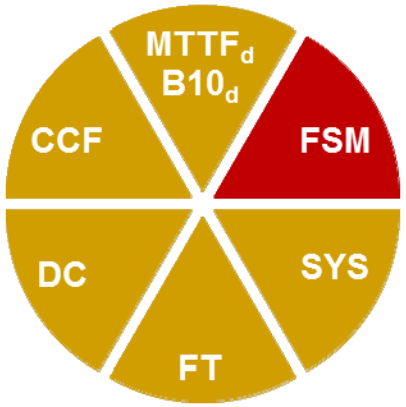



CAPIEL
european coordinating committee of manufacturers of electrical switchgear and controlgear

# Who, what, when?

- **Is there a need for risk reduction at the machine level?**
- **Can we  achieve this risk reduction with a control system function?**
- **Do we have sufficient competencies and human resources?**
- **Is there a clear and documented project plan for safety including Validation?**
- **Does everyone know what their tasks and responsibilities are?**
- **Is this all we need???**

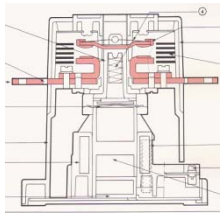


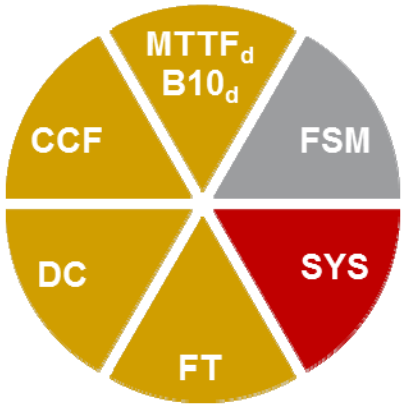

**FSM = Functional safety management**

CAPIEL
european coordinating committee of manufacturers of electrical switchgear and controlgear

# What about systematic failure?

- **Is power ratings, utilisation category, vibration, shock, overvoltage, environment, durability and short-circuit coordination taken into account?**
- **If you change the motor from IE1 to IE3 and install a new transformer, is the contactor still suitable for this application?**
- **Is this all we need?**



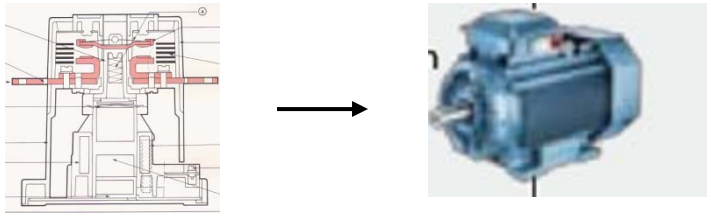


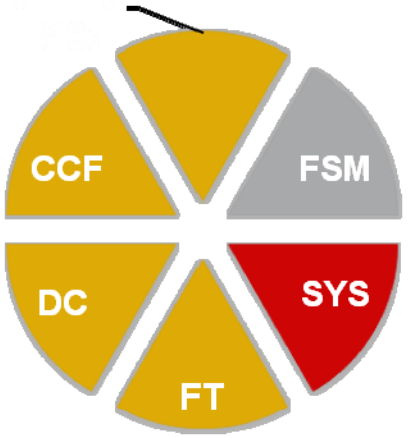

**SYS =Systematic integrity**

CAPIEL
european coordinating committee of manufacturers of electrical switchgear and controlgear

# How often will it operate?

- **Only when something is wrong and someone pushes the emergency switch**
- **Every day when the machine is turned off**
- **Every machine cycle**
- **On Regular maintenance tests**

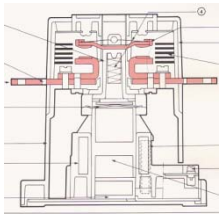


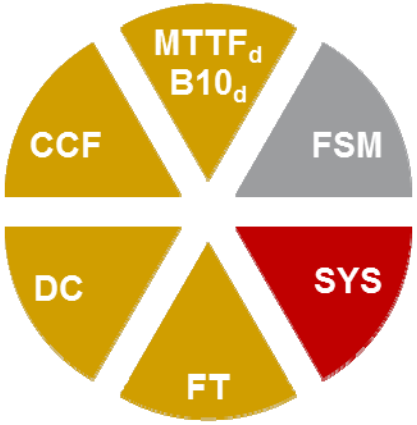



CAPIEL
european coordinating committee of manufacturers of electrical switchgear and controlgear

# How often will it operate?

- **High demand means more than one operation/year – main reasons to fault is “wear out” (e.g.: parts break)**
- **Low demand means less than once a year – main reasons to fault is “ageing” (e.g.: lubrication get sticky, plastic get fragile)**
- **Continuous mode means safety function is part of normal operation and retains equipment in a safe state**

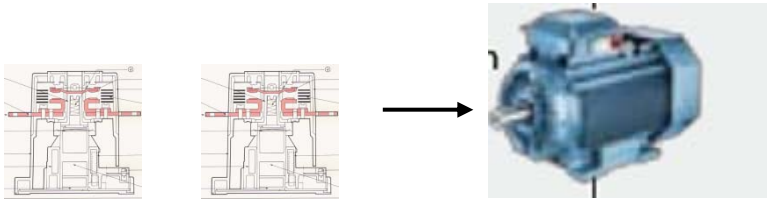


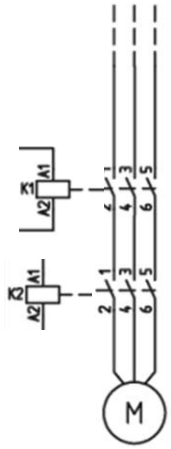


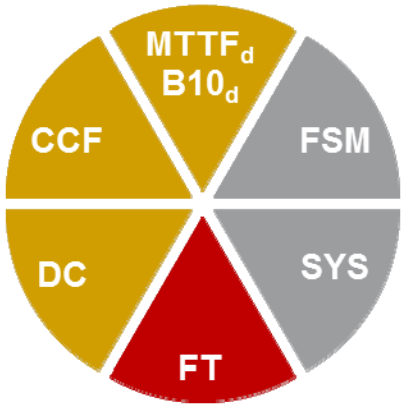

CAPIEL
european coordinating committee of manufacturers of electrical switchgear and controlgear

# Do We Need Two?

- **Do we need 2 contactors?**
- **High risk – we might need two…**





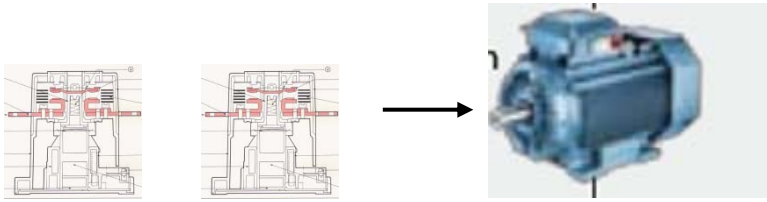



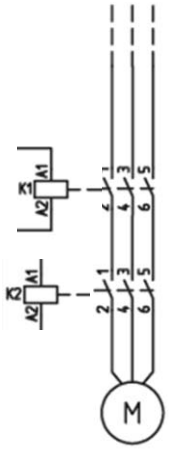

**FT = Fault tolerant**

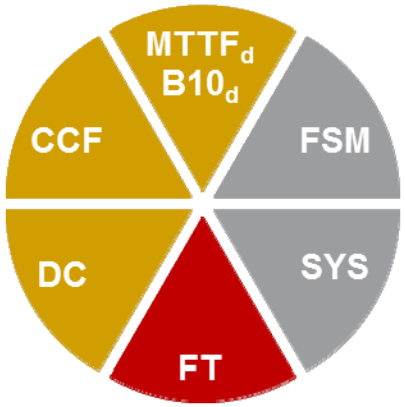
CAPIEL
european coordinating committee of manufacturers of electrical switchgear and controlgear

# What If One Fails

- **If one fails – do we know?**
- **Do we need to know??**
- **In this case we have no diagnostics and the fault is not detected**
- **Without diagnostics we might continue to use the machine until a second fault occurs.**





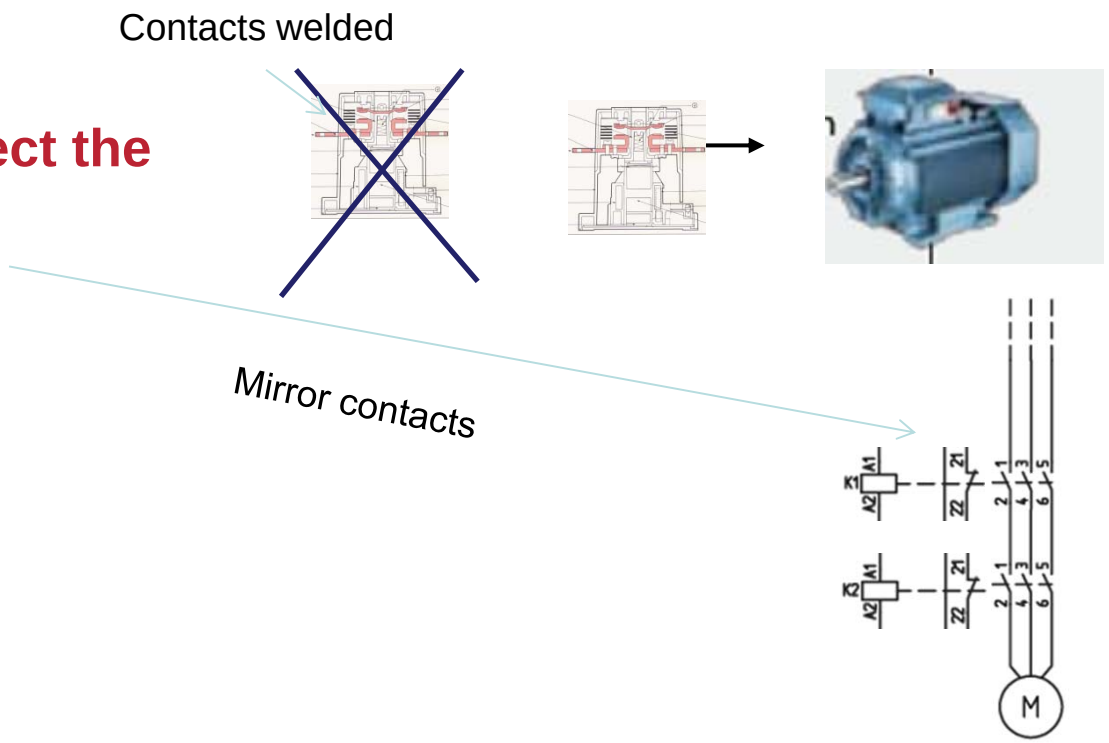



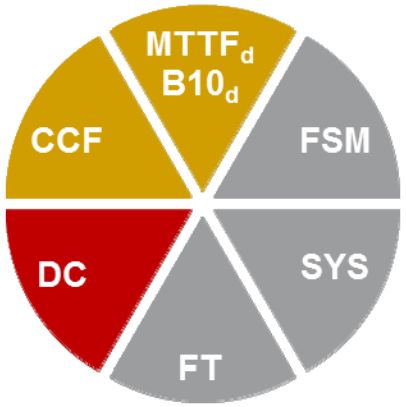

FT **= Fault Tolerance**

CAPIEL
european coordinating committee of manufacturers of electrical switchgear and controlgear

# Diagnostic Coverage

- **Diagnostics can detect the first fault**



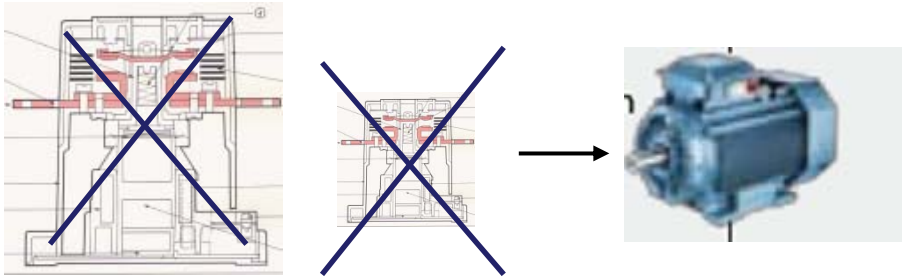



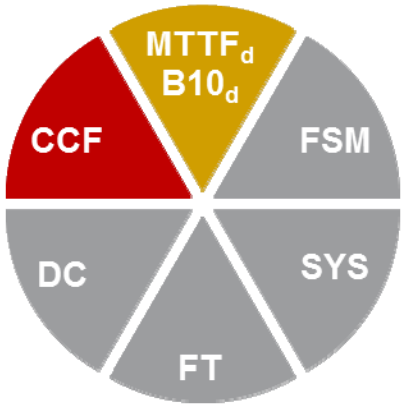

DC **= Diagnostic Coverage**

CAPIEL
european coordinating committee of manufacturers of electrical switchgear and controlgear

# Common Cause Failure

- **What happens if they both fail at the same time?**





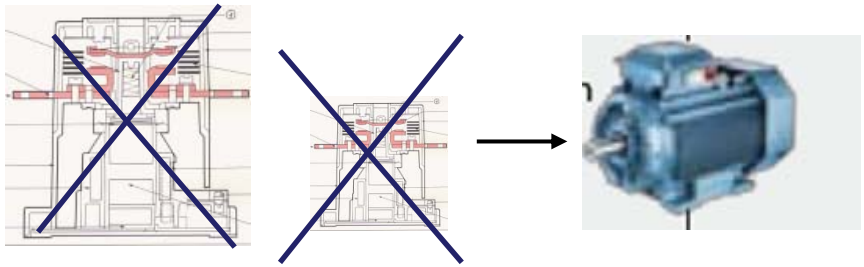

**CCF = Common cause failure**

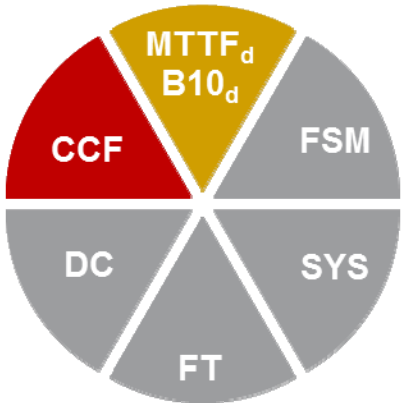
CAPIEL
european coordinating committee of manufacturers of electrical switchgear and controlgear

# Common Cause Failure

- **One means of addressing CCF is to adopt diversity and over-dimensioning**

CB





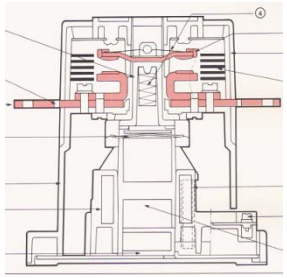

Mirror contacts indicate fault and Safety PLC or safety relay will send signal to CB to open

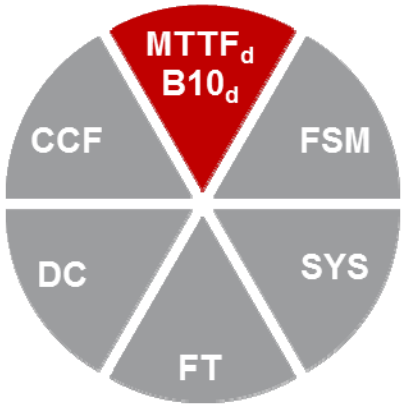
**CCF = Common cause failure**

CAPIEL
european coordinating committee of manufacturers of electrical switchgear and controlgear

# How Good Is It??

- **What is the reliability of these contactors?**
- **Which is the most suitable to my application?**
- **Component/sub-system standard must address functional safety applications**
- **See IEC 60947-4-1 Annex K**

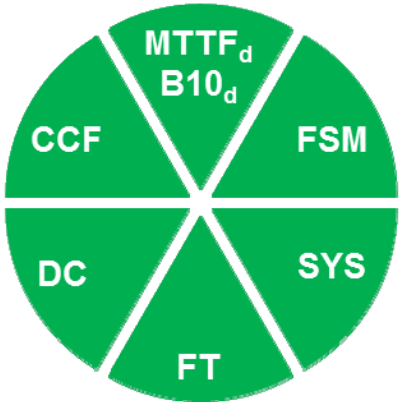





**$MTTF_d$ = Mean time to a dangerous failure**

CAPIEL
european coordinating committee of manufacturers of electrical switchgear and controlgear

# The abbreviations…




**If any of the points listed above aren't dealt with properly we could fail to achieve our goal of a functionally safe system.**

- **$B10_d$ – Number of cycles until 10% of** devices have Dangerous Failure
- **$MTTF_d$ – Mean Time To Dangerous Failure**

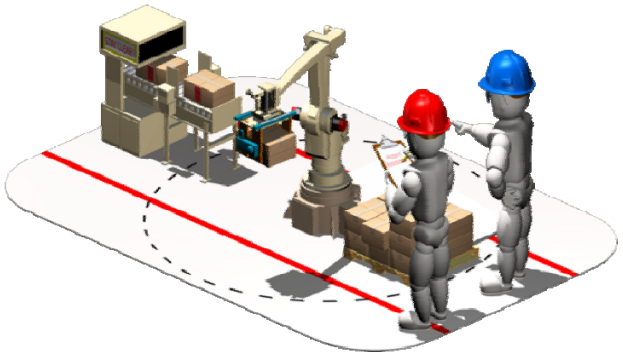
$$MTTF_d = \frac{B10_d}{0.1 \times Cycles/year}$$

- **FT – Fault Tolerance**
- **$DC_{avg}$ – Diagnostic Coverage**
- **CCF – Common Cause Failure**
- **SYS – Systematic Integrity**
- **FSM – Functional Safety Management**

CAPIEL
european coordinating committee of manufacturers of electrical switchgear and controlgear

# Functional safety benefits

- **Integration of functional safety into the global design leads to:**
  - More safe and productive machine
  - Reduction of the life cycle cost both for the machine and the operation
  - Better integration of the safety control system design within the machine design process

CAPIEL
european coordinating committee of manufacturers of electrical switchgear and controlgear

# What is necessary for machine builders?

- Definition of the failure modes
- Reliability data e.g. B10 and failure mode ratio, $MTTF_d$
- Maintenance aspects: to be integrated in the instruction manual
- Utilisation categories
- Integration constraint
- Reliability data should be given in accordance with a relevant international standard, e.g. for contactors, IEC 60947-4-1 Annex K
- CAPIEL has published default values for B10 and failure mode ratios and $MTTF_d$ that can be used where more precise data is not given by the manufacturer

CAPIEL
european coordinating committee of manufacturers of electrical switchgear and controlgear