



## **Risk**

# **Failure is an Option**

**Doug Phillips**  
**American Global Maritime**

*October 9-10, 2007*

# FAILURE IS AN OPTION

**Doug Phillips**



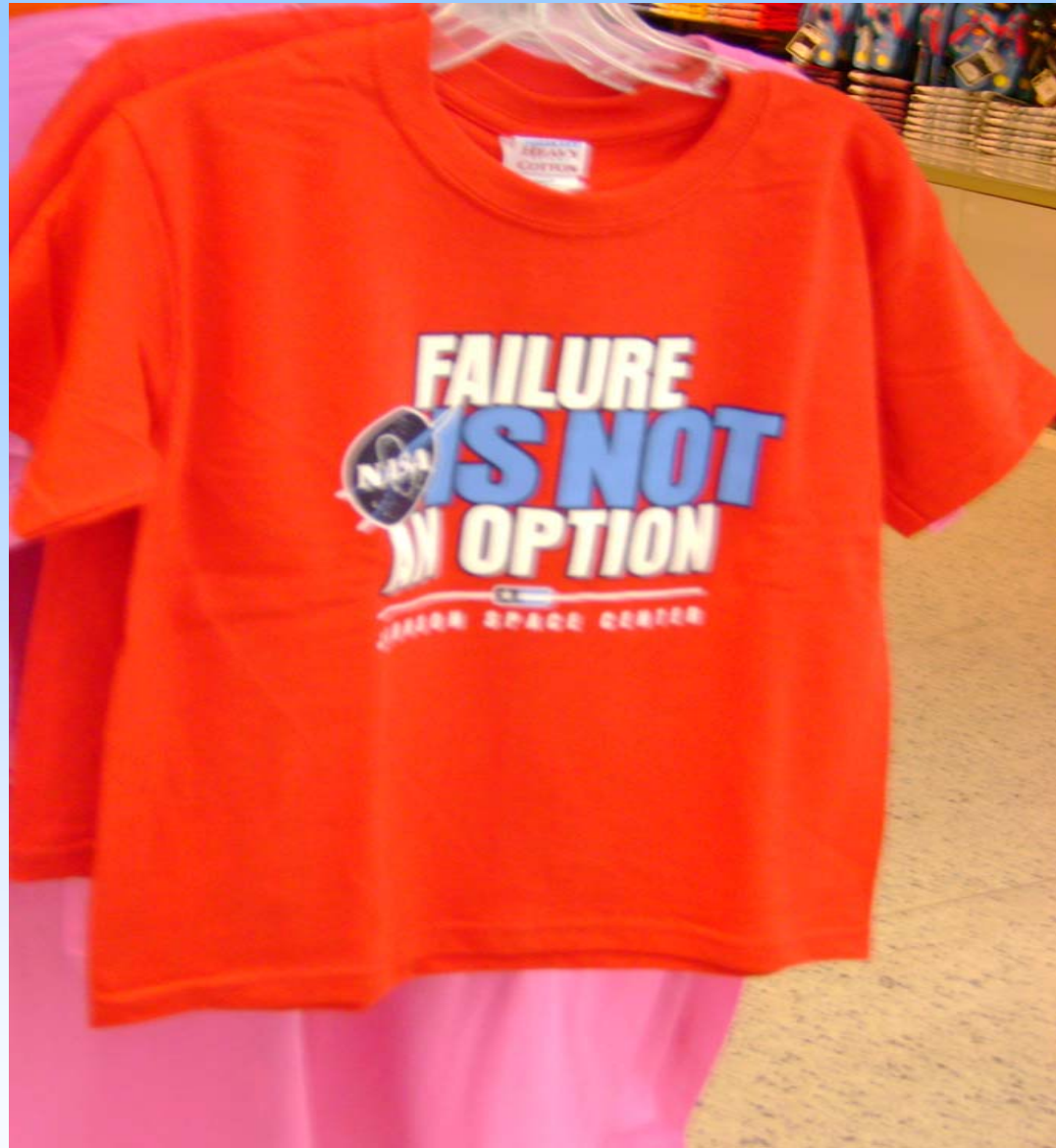


# Introduction

- What is a failure - recap?
- Happening in practice - trying to make it fault tolerant not independent
- Some examples
- Conclusions

# NASA MOTTO











# DP - 'Failure is an option' - IMO

# DP - ‘Failure is an option’ - IMO

- **For equipment class 2**, a loss of position is not to occur in the event of a **single fault** in any **active component or system**.

Normally static components will not be considered to fail where adequate protection from damage is demonstrated, and reliability is to the satisfaction of the Administration.

# DP - 'Failure is an option' - IMO

# DP - 'Failure is an option' - IMO

- Single failure criteria include:

# DP - 'Failure is an option' - IMO

- Single failure criteria include:
- Any active component or system

# DP - 'Failure is an option' - IMO

- **Single failure criteria include:**
- Any active component or system
- Any normally static component (cables, pipes manual valves, etc.) which is not properly documented with respect to protection and reliability.

# DP - 'Failure is an option' - IMO

# DP - 'Failure is an option' - IMO

- **For equipment class 3, a single failure as class 2, and any normally static component** is assumed to fail.

# DP - ‘Failure is an option’ - IMO

- **For equipment class 3, a single failure as class 2, and any normally static component** is assumed to fail.
- All components in any one watertight comp, from fire or flooding.

# DP - 'Failure is an option' - IMO

- **For equipment class 3, a single failure as class 2, and any normally static component** is assumed to fail.
- All components in any one watertight comp, from fire or flooding.
- All components in any one fire sub-division, from fire or flooding

# DP - 'Failure is an option' - IMO

- **For equipment class 3, a single failure as class 2, and any normally static component** is assumed to fail.
- All components in any one watertight comp, from fire or flooding.
- All components in any one fire sub-division, from fire or flooding
- For equipment classes 2 and 3, a **single inadvertent act** should be considered as a single fault if such an act is reasonably probable.

# DP - 'Failure is an option' – FMEA

# DP - 'Failure is an option' – FMEA

- Analysis to find all single failures

# DP - 'Failure is an option' – FMEA

- Analysis to find all single failures
- Independent systems

# DP - 'Failure is an option' – FMEA

- Analysis to find all single failures
- Independent systems
- Trials to test single failures

# DP - 'Failure is an option' – FMEA

- Analysis to find all single failures
- Independent systems
- Trials to test single failures
- Annual trials to reaffirm redundancy

# DP - 'Failure is an option' – FMEA

- Analysis to find all single failures
- Independent systems
- Trials to test single failures
- Annual trials to reaffirm redundancy
- Updated after – modifications, DP incidents, industry experience

# DP - 'Failure is an option' – FMEA

- Analysis to find all single failures
- Independent systems
- Trials to test single failures
- Annual trials to reaffirm redundancy
- Updated after – modifications, DP incidents, industry experience
- Software modification management

# DP - 'Failure is an option' – FMEA

- Analysis to find all single failures
- Independent systems
- Trials to test single failures
- Annual trials to reaffirm redundancy
- Updated after – modifications, DP incidents, industry experience
- Software modification management
- **Hardware modification management**

# In Practice

# In Practice

- Designers and crew not comfortable with **‘thinking failure’**

# In Practice

- Designers and crew not comfortable with **‘thinking failure’**
- Include back ups, work around, c’overs, cross feeds etc etc.

# In Practice

- Designers and crew not comfortable with **‘thinking failure’**
- Include back ups, work around, c’overs, cross feeds etc etc.
- Try to make it **fault tolerant**

# In Practice

- Designers and crew not comfortable with **‘thinking failure’**
- Include back ups, work around, c’overs, cross feeds etc etc.
- Try to make it **fault tolerant**
- Propulsion principle – get home

# In Practice

- Designers and crew not comfortable with **‘thinking failure’**
- Include back ups, work around, c’overs, cross feeds etc etc.
- Try to make it **fault tolerant**
- Propulsion principle – get home
- Very often on site modification or ‘improvements’

# In Practice

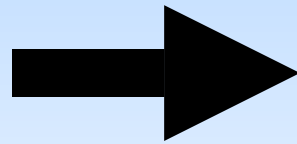
- Designers and crew not comfortable with **‘thinking failure’**
- Include back ups, work around, c’overs, cross feeds etc etc.
- Try to make it **fault tolerant**
- Propulsion principle – get home
- Very often on site modification or ‘improvements’
- **And of course my favorite the dreaded**

# In Practice

- **DIODE OR!!!!!!!**

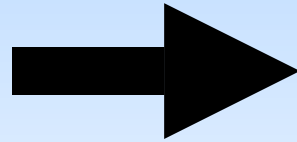
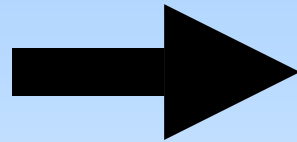
# In Practice

- **DIODE OR!!!!!!!**



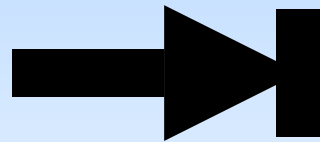
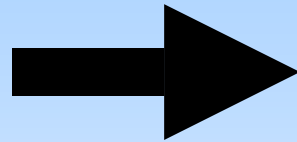
# In Practice

- **DIODE OR!!!!!!!**



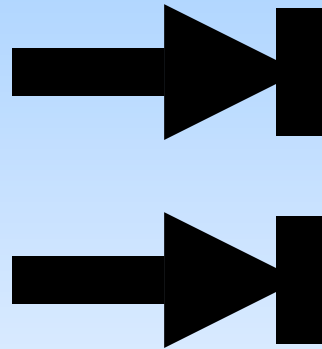
# In Practice

- **DIODE OR!!!!!!!**



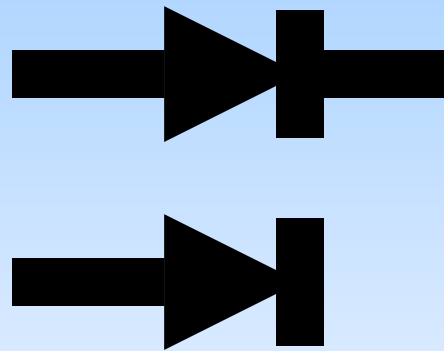
# In Practice

- **DIODE OR!!!!!!!**



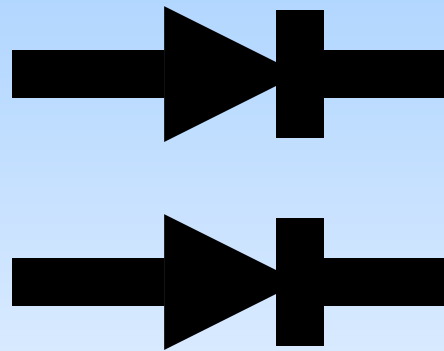
# In Practice

- **DIODE OR!!!!!!!**



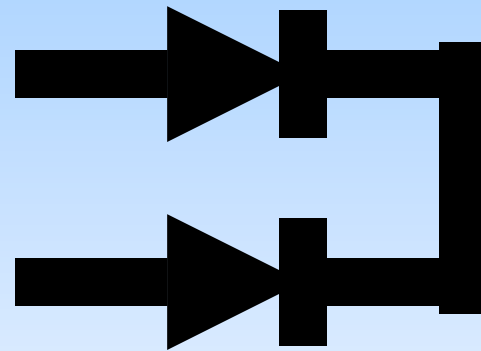
# In Practice

- **DIODE OR!!!!!!!**



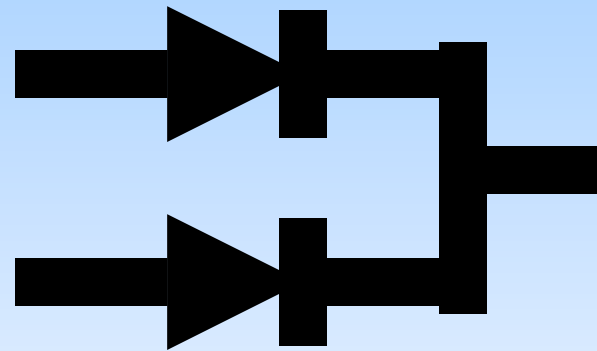
# In Practice

- **DIODE OR!!!!!!!**



# In Practice

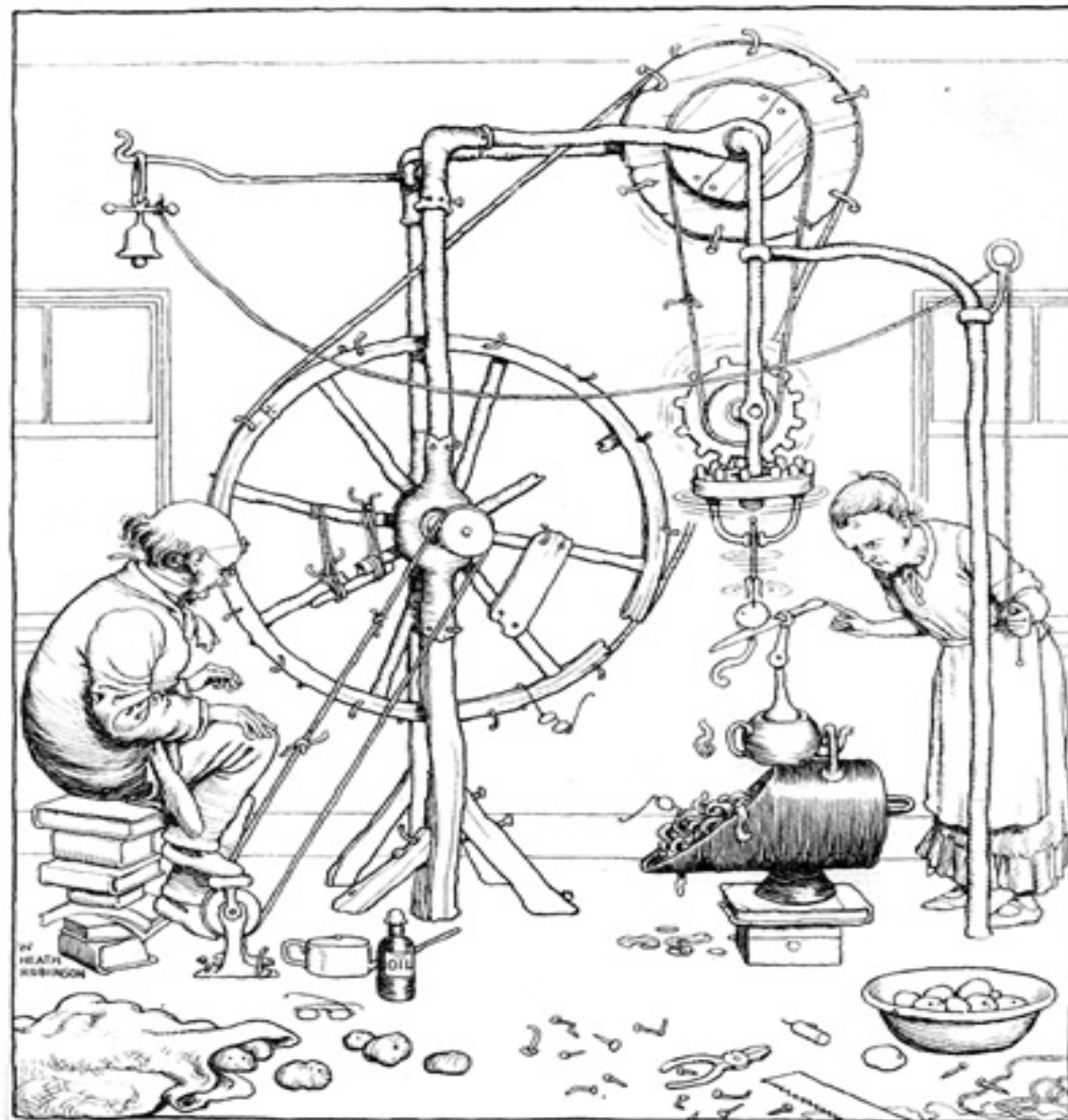
- **DIODE OR!!!!!!!**



# Before Electrical Examples

- Rube Goldman
- Heath Robinson
- **Wallace and Grommit – cracking contraptions**
- All mechanical classic over designs
- No electrical ones – except on DP ships
- One electro mechanical one

# All Mechanical



The Professor's invention for peeling potatoes.

# Electro Mechanical

June 8, 1965

Filed March 14, 1961

H. L. SHATTO, JR., ET AL  
SHIP CONTROL SYSTEM

3,187,704

3 Sheets-Sheet 2

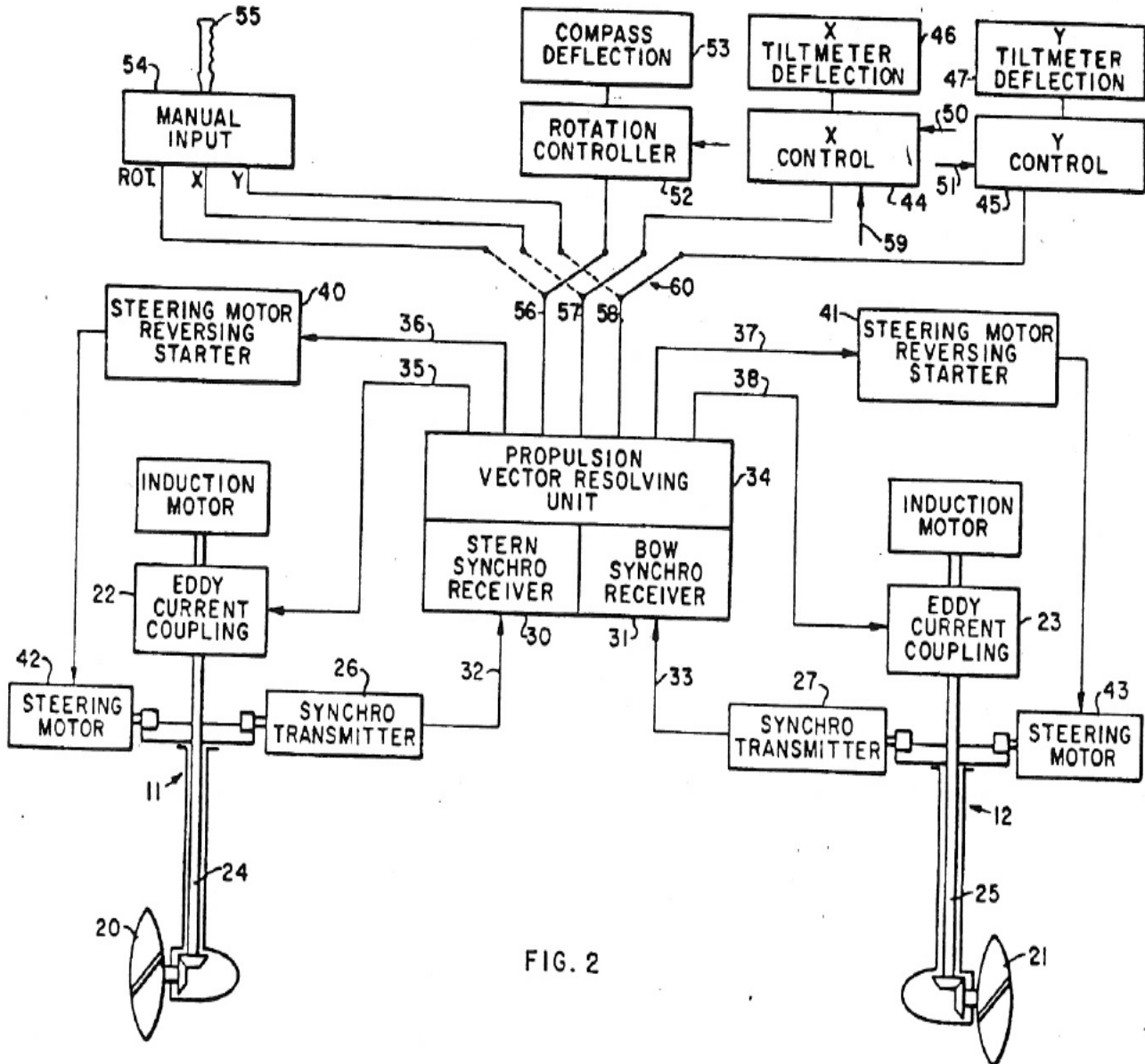


FIG. 2

INVENTORS:

H. L. SHATTO JR.

J. R. DOZIER

BY: *Thomas S. Baird*  
THEIR ATTORNEY

7 am. - 11  
 1 in P 9205; Kolb

June 8, 1965 H. L. SHATTO, JR., ET AL 3,187,704  
 SHIP CONTROL SYSTEM  
 Filed March 14, 1961 3 Sheets-Sheet 1

*Shell Oil Co.*

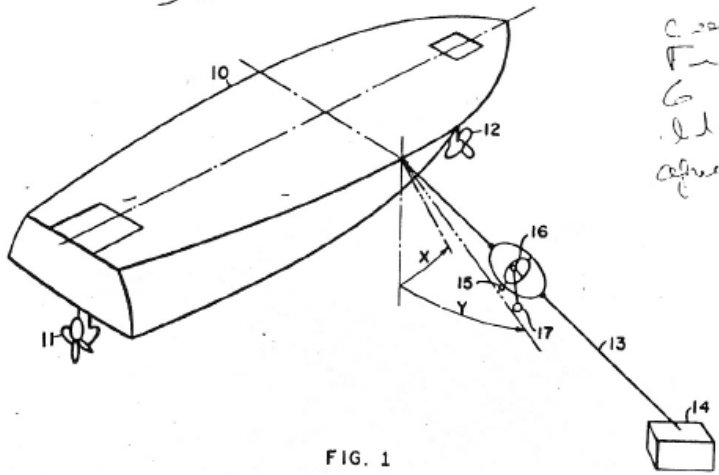


FIG. 1

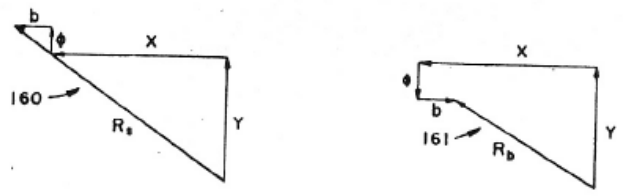


FIG. 4

INVENTORS:  
 H. L. SHATTO JR.  
 J. R. DOZIER  
 BY: *Sheldon E. Bittel*  
 THEIR ATTORNEY

Return to Session Directory

June 8, 1965 H. L. SHATTO, JR., ET AL 3,187,704  
 SHIP CONTROL SYSTEM

Filed March 14, 1961 3 Sheets-Sheet 3

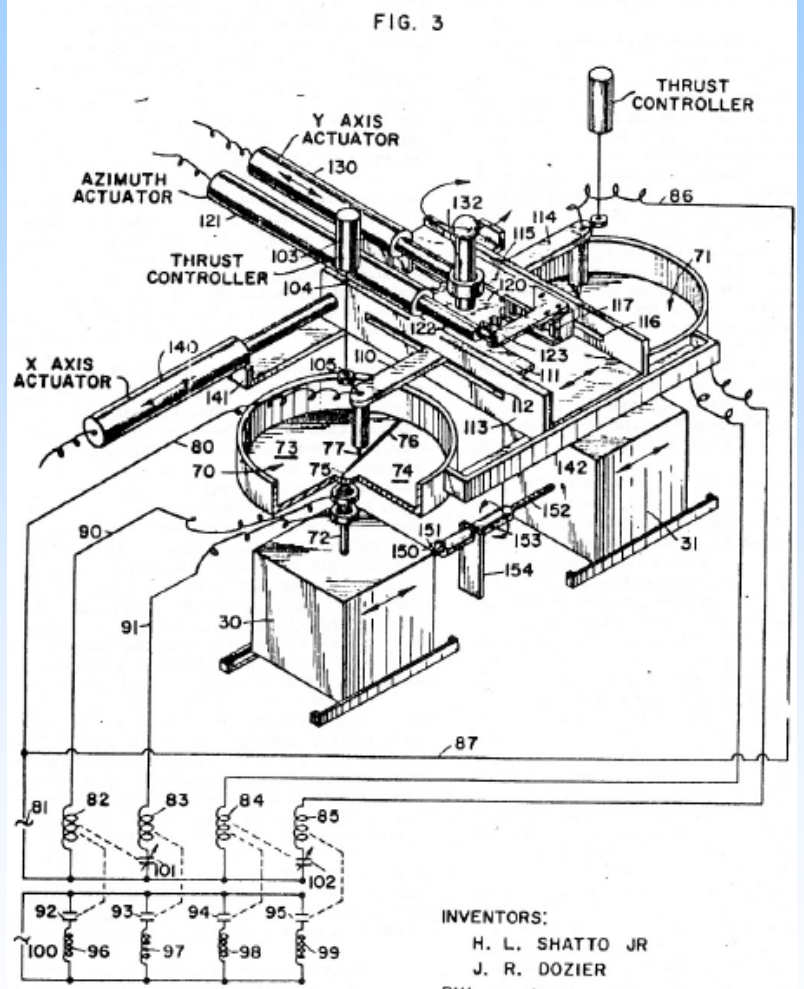


FIG. 3

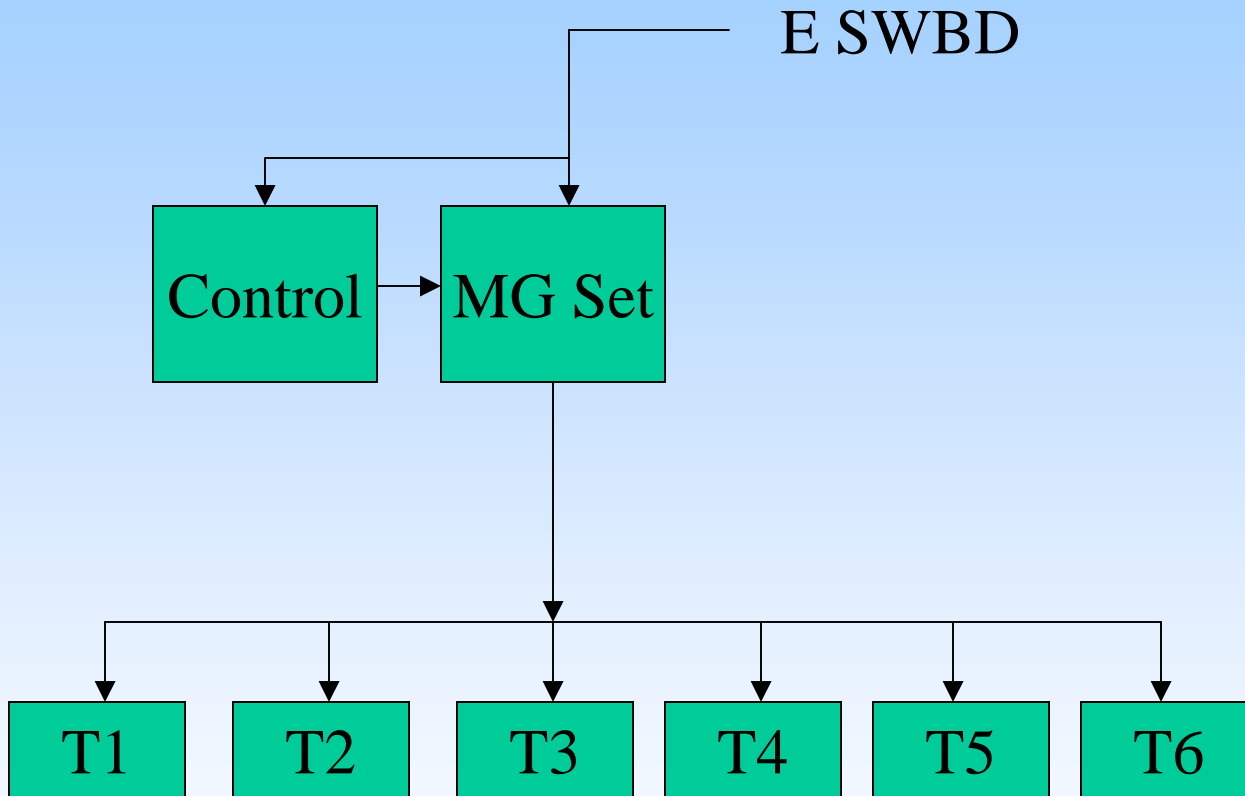
INVENTORS:  
 H. L. SHATTO JR.  
 J. R. DOZIER  
 BY: *Sheldon E. Bittel*  
 THEIR ATTORNEY

# Electrical Examples from Experience

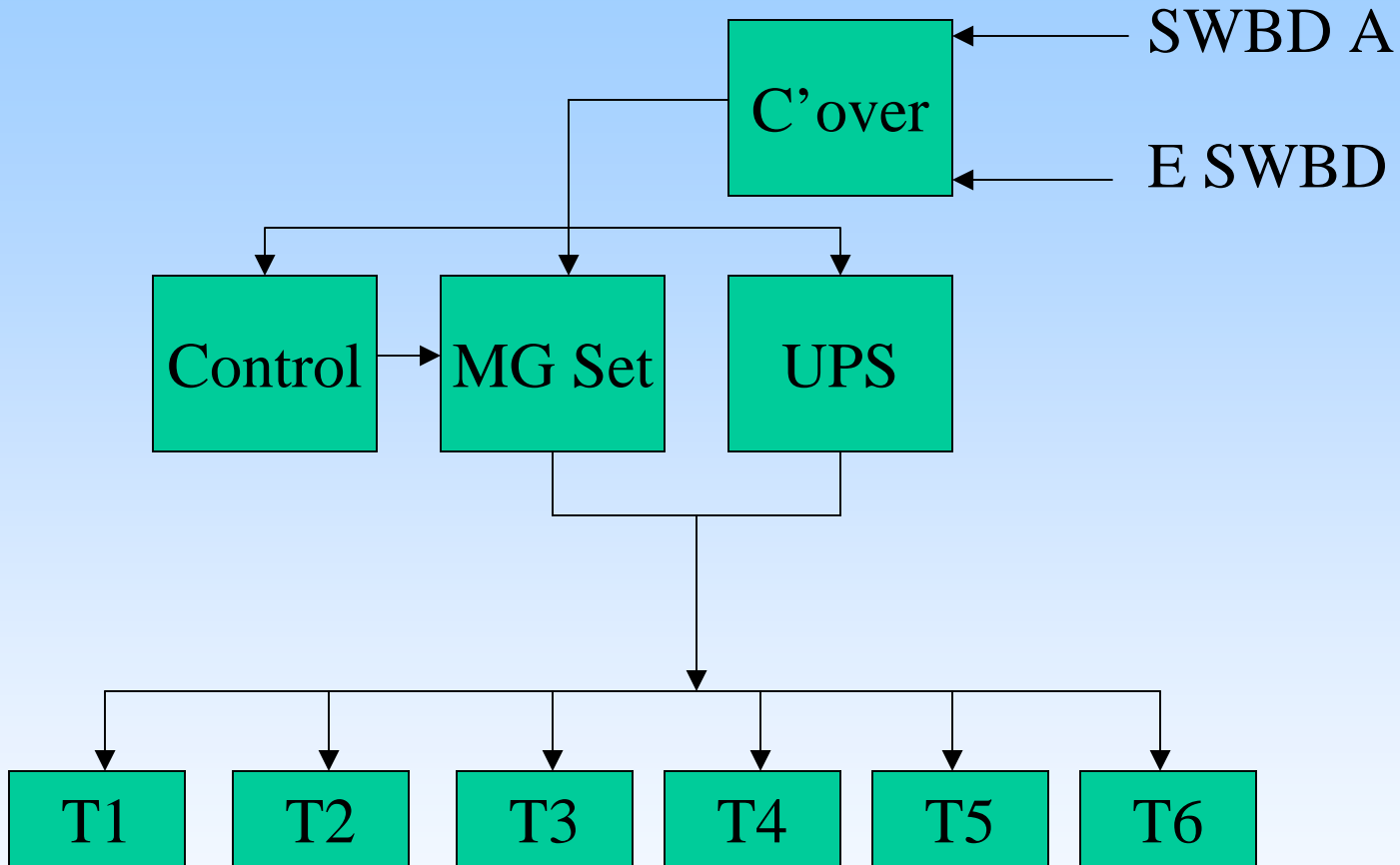
## 9 Examples (plus 1)

- block diagrams to keep it simple
- all DP vessels – mainly modification but not all
- *the thought process all my own*
- All well intentioned

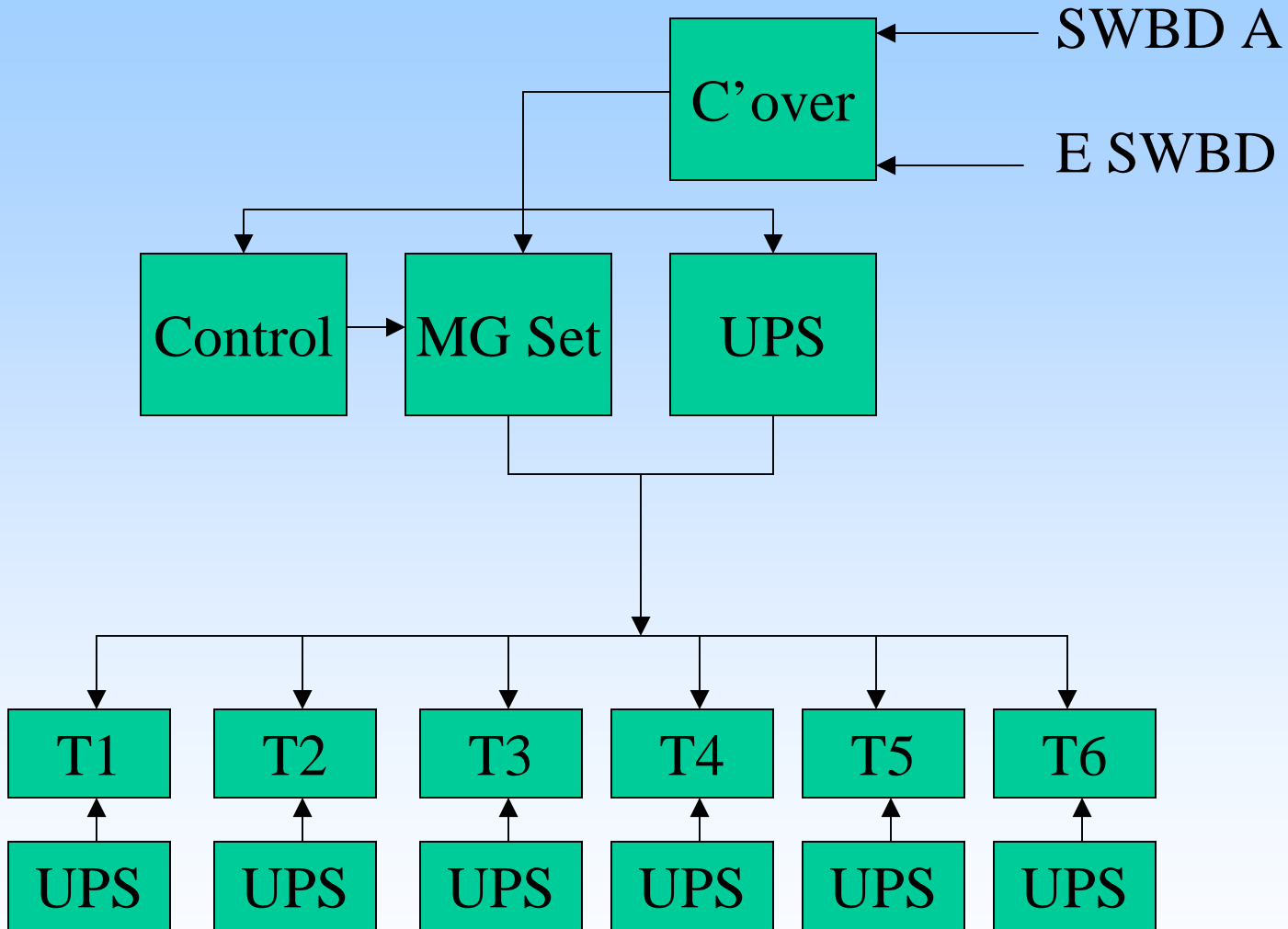
# Example 1 - 'Clean Supply'



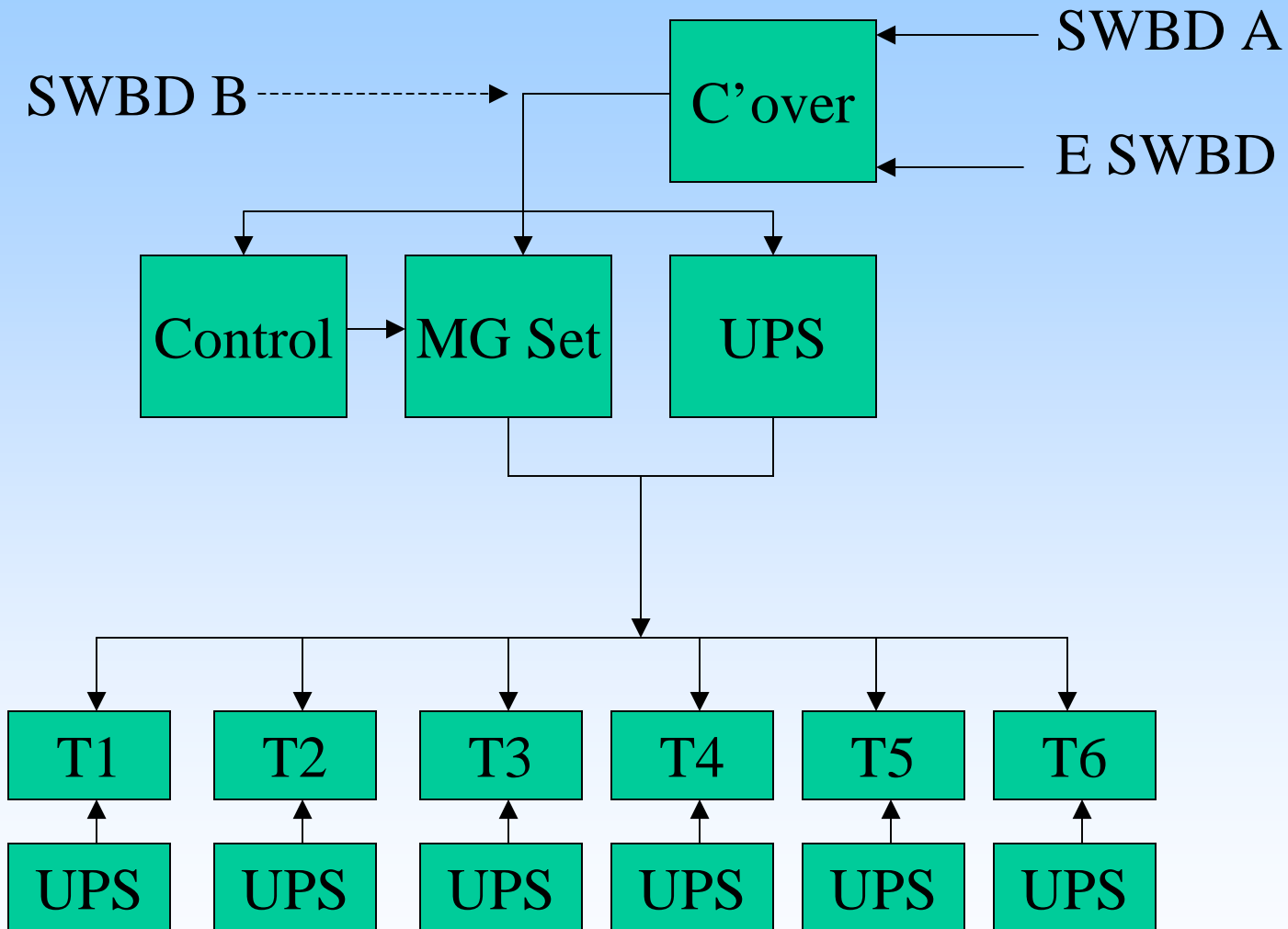
# Example 1 - 'Clean Supply'



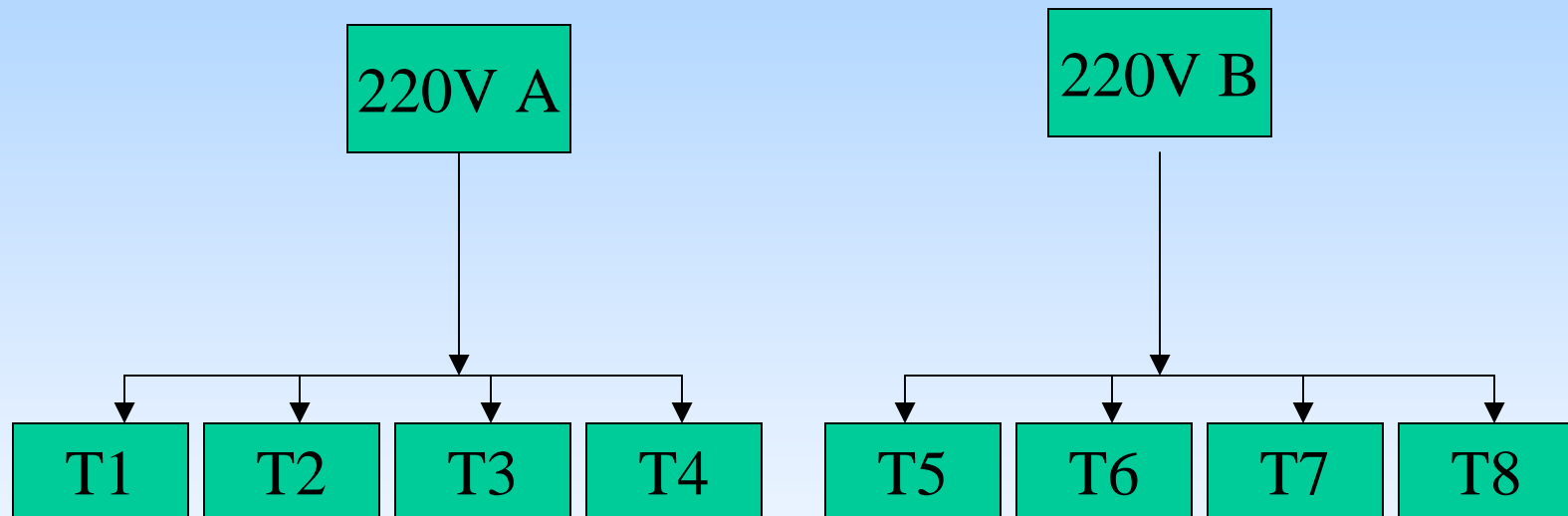
# Example 1 - 'Clean Supply'



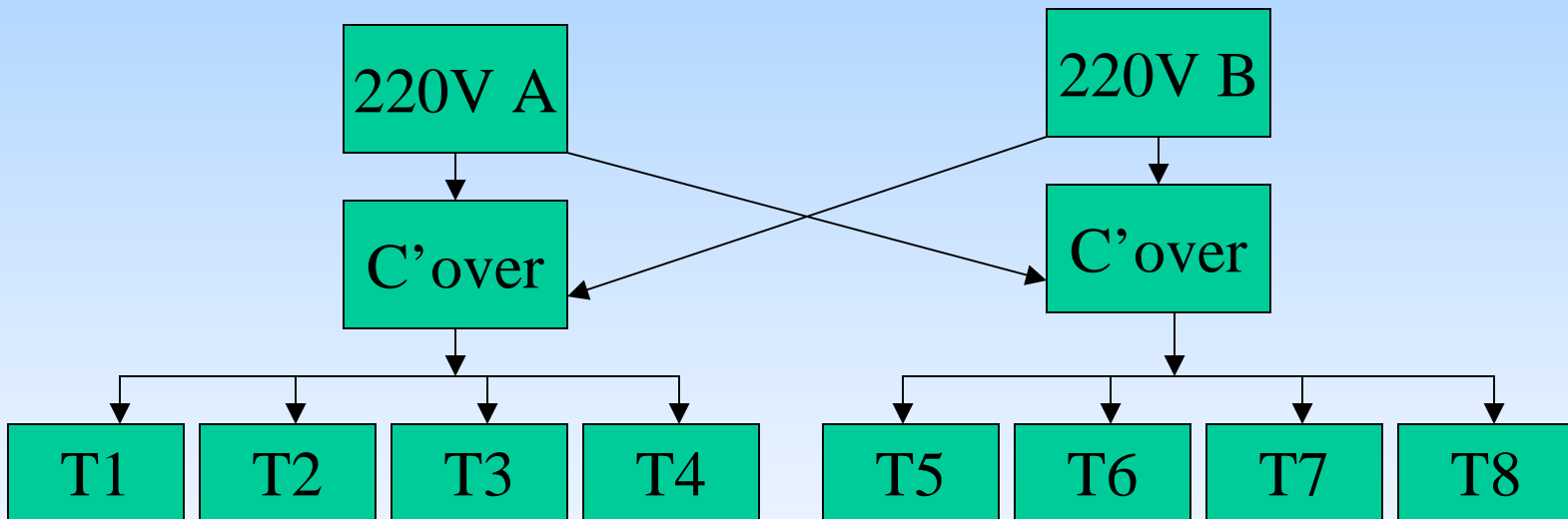
# Example 1 - 'Clean Supply'



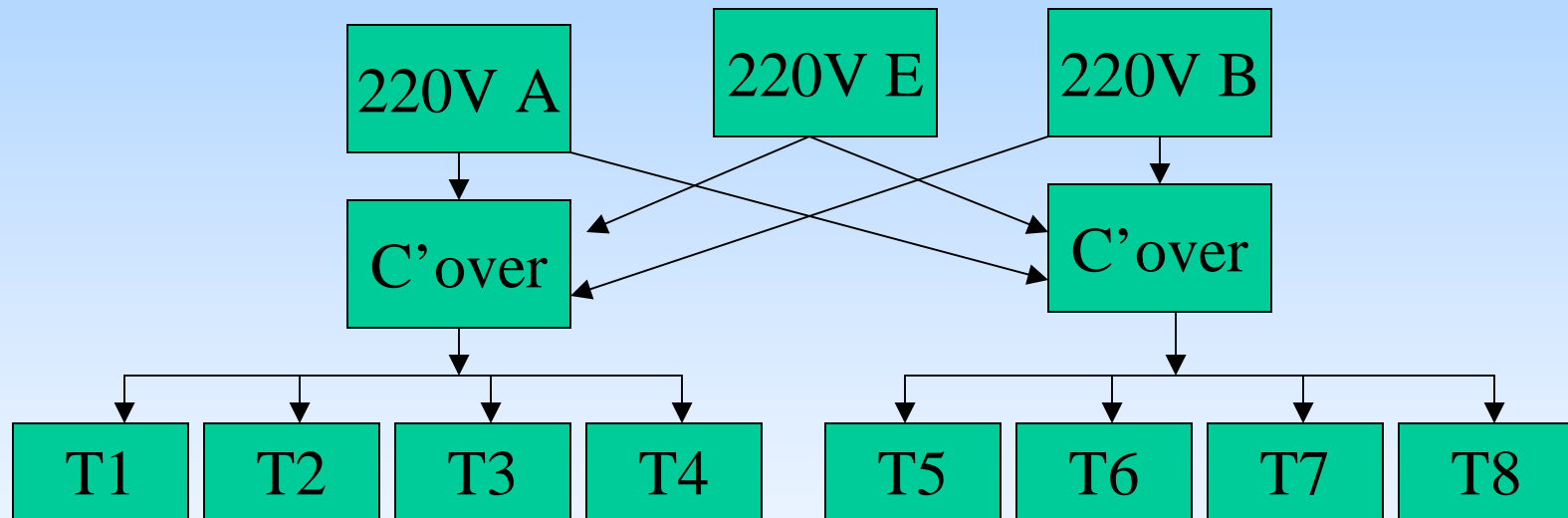
# Example 2 - “Back Up Supplies”



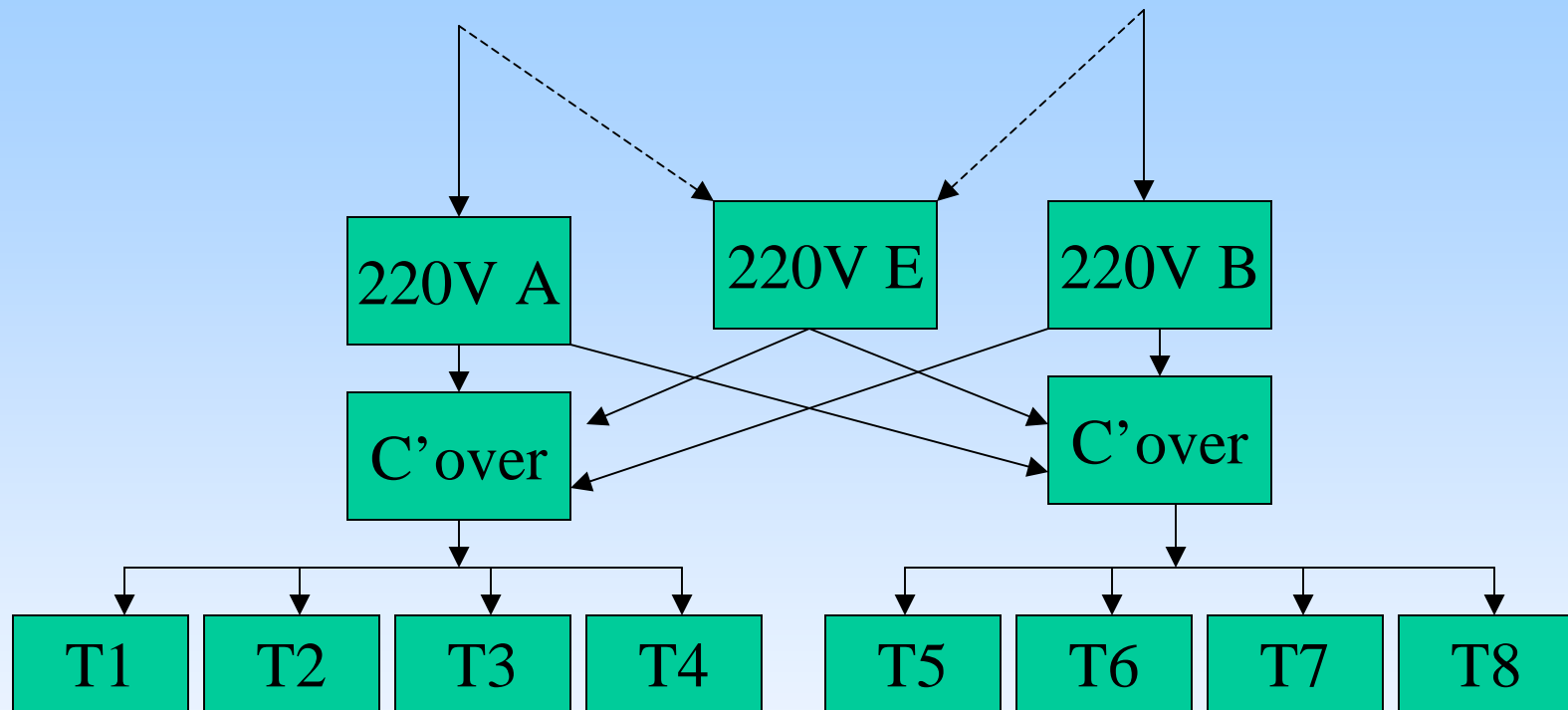
# Example 2 - “Back Up Supplies”



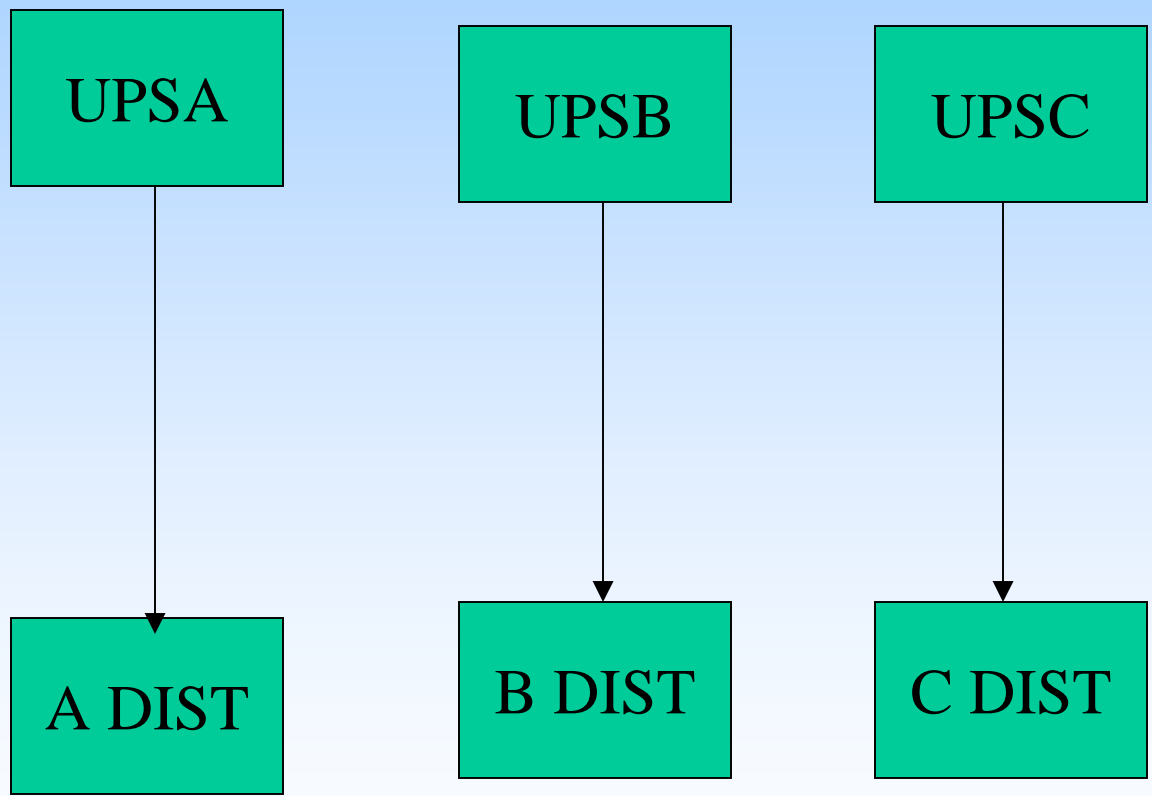
# Example 2 - “Back Up Supplies”



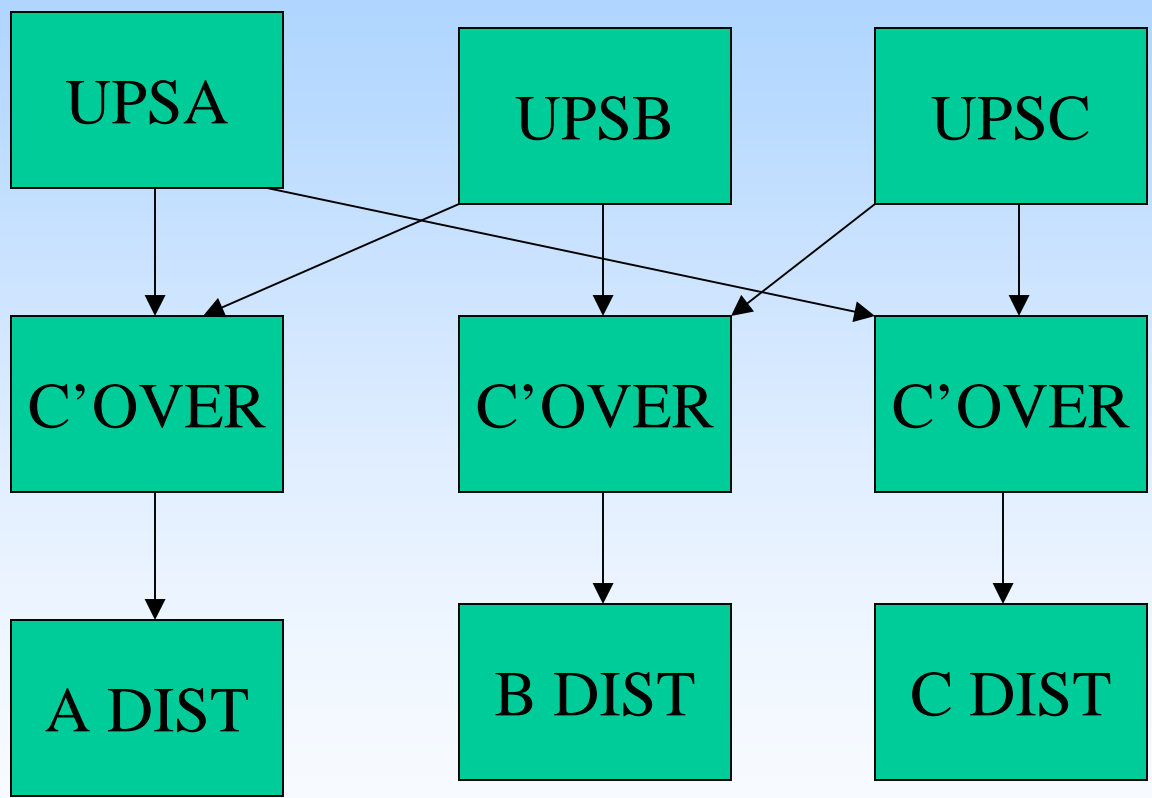
# Example 2 - “Back Up Supplies”



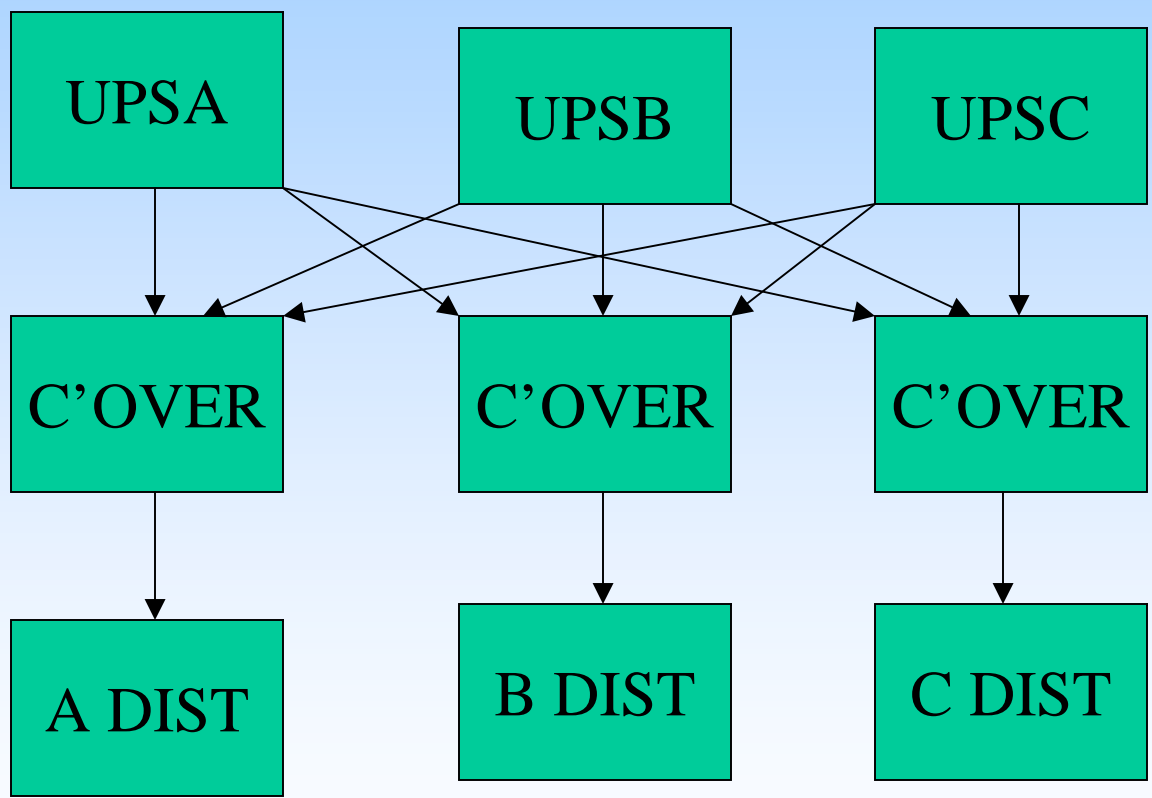
# Example 3 - UPS's's's



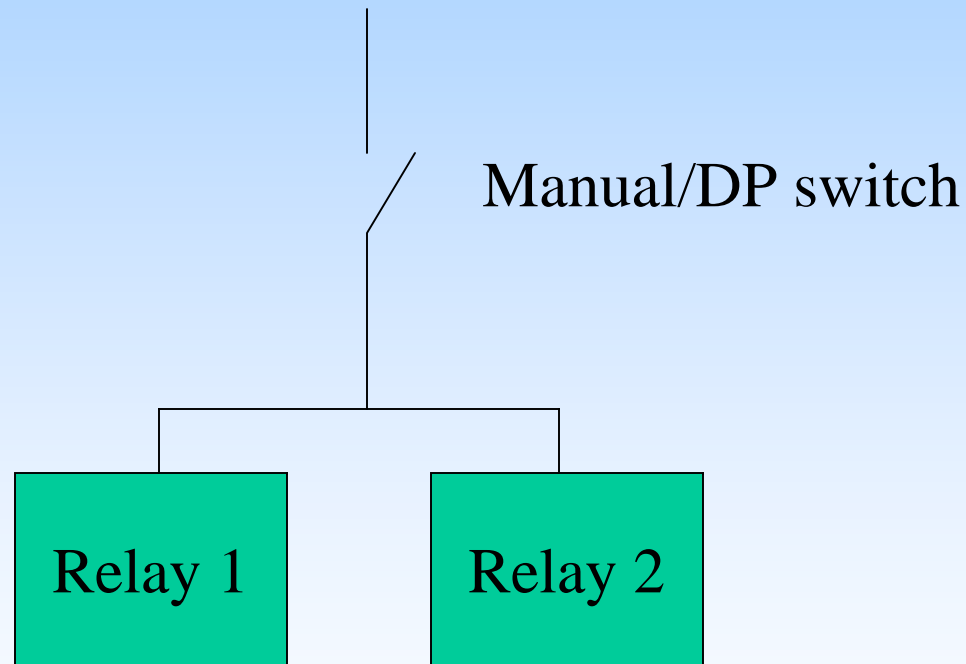
# Example 3 - UPS's's's



# Example 3 - UPS's's's



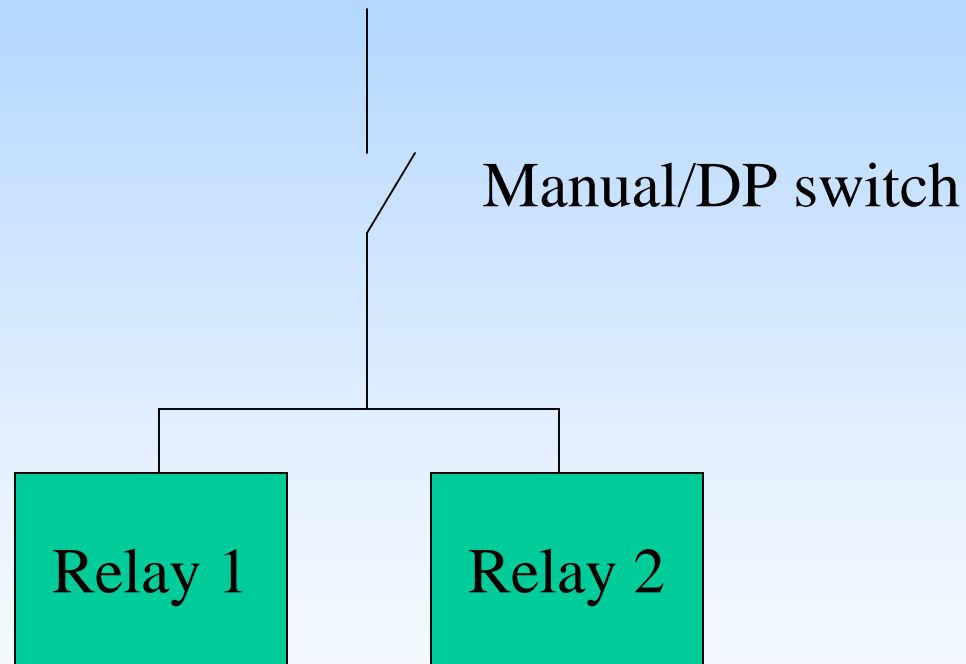
# Example 4 - Top of Class 3



Half thrusters  
select to DP

Half thrusters  
select to DP

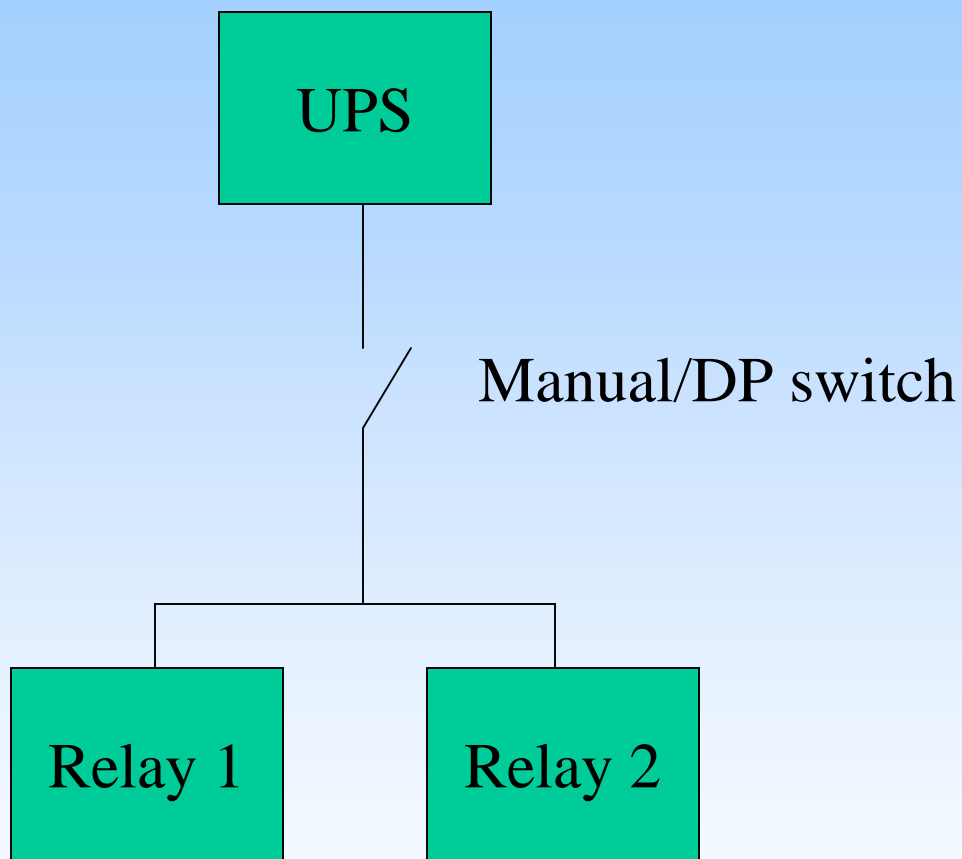
# Example 4 - Top of Class 3



Half thrusters  
select to DP

Half thrusters  
select to DP

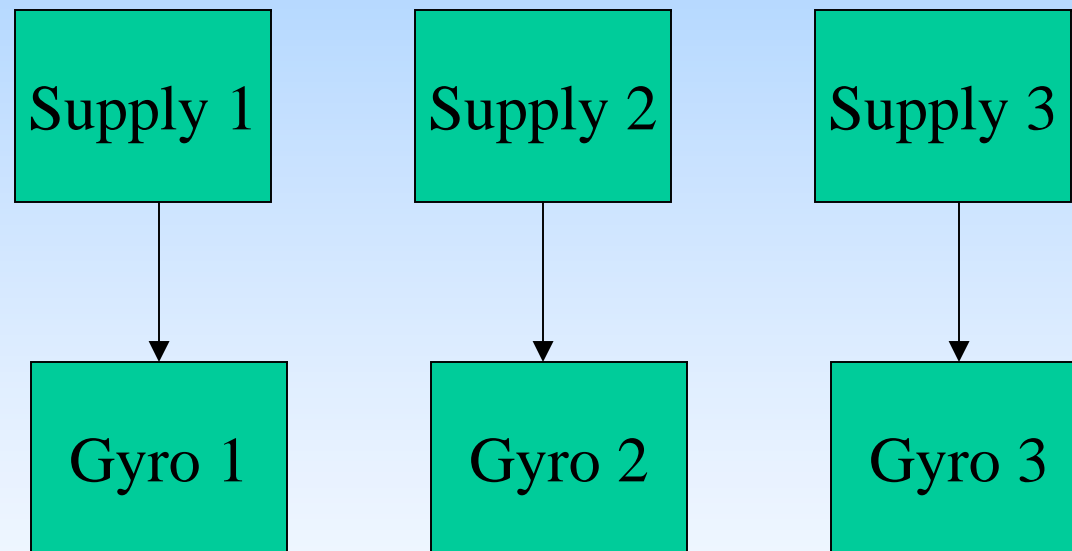
# Example 4 - Top of Class 3



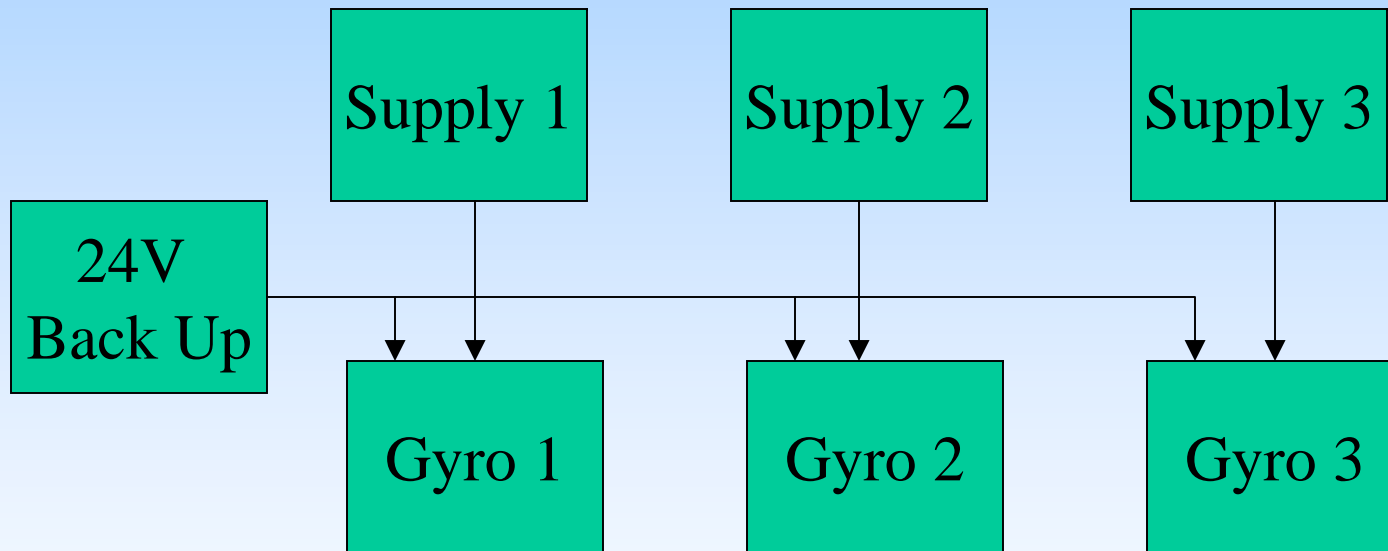
Half thrusters  
select to DP

Half thrusters  
select to DP

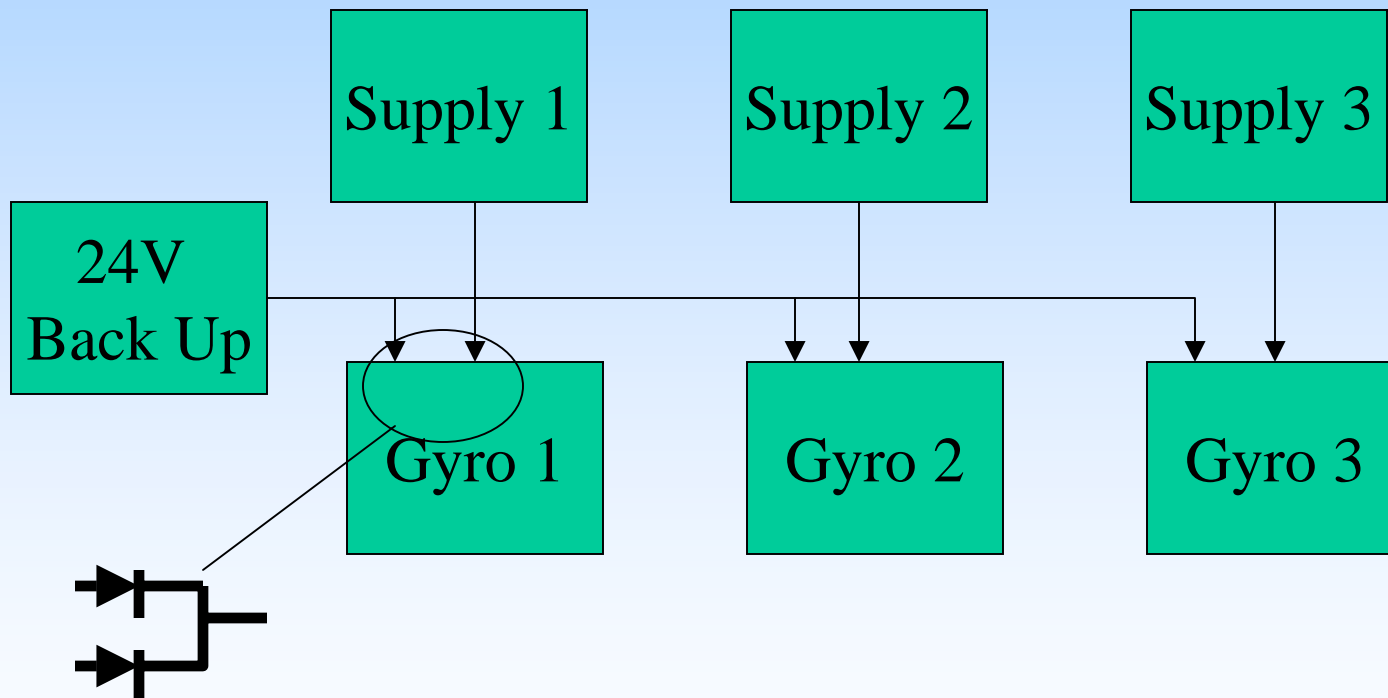
# Example 5 - 'Backed up' Gyros



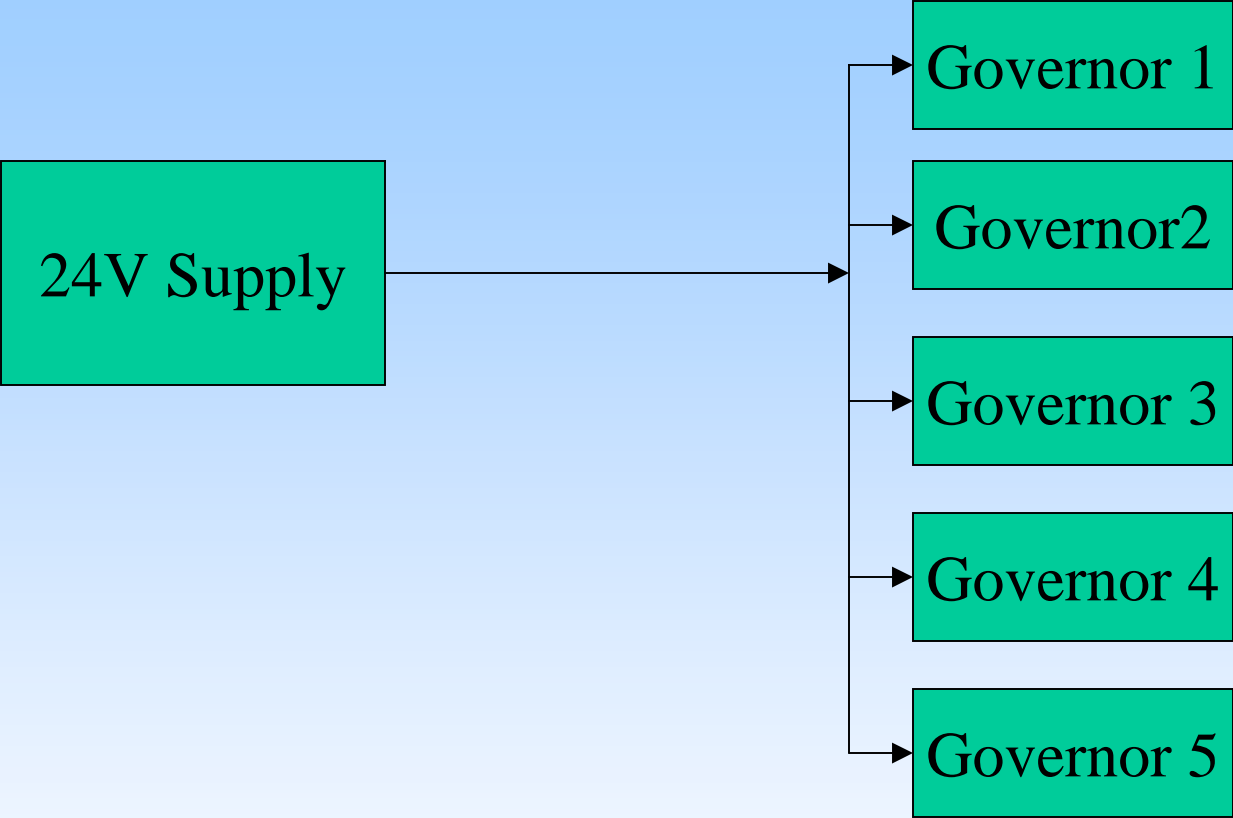
# Example 5 - 'Backed up' Gyros



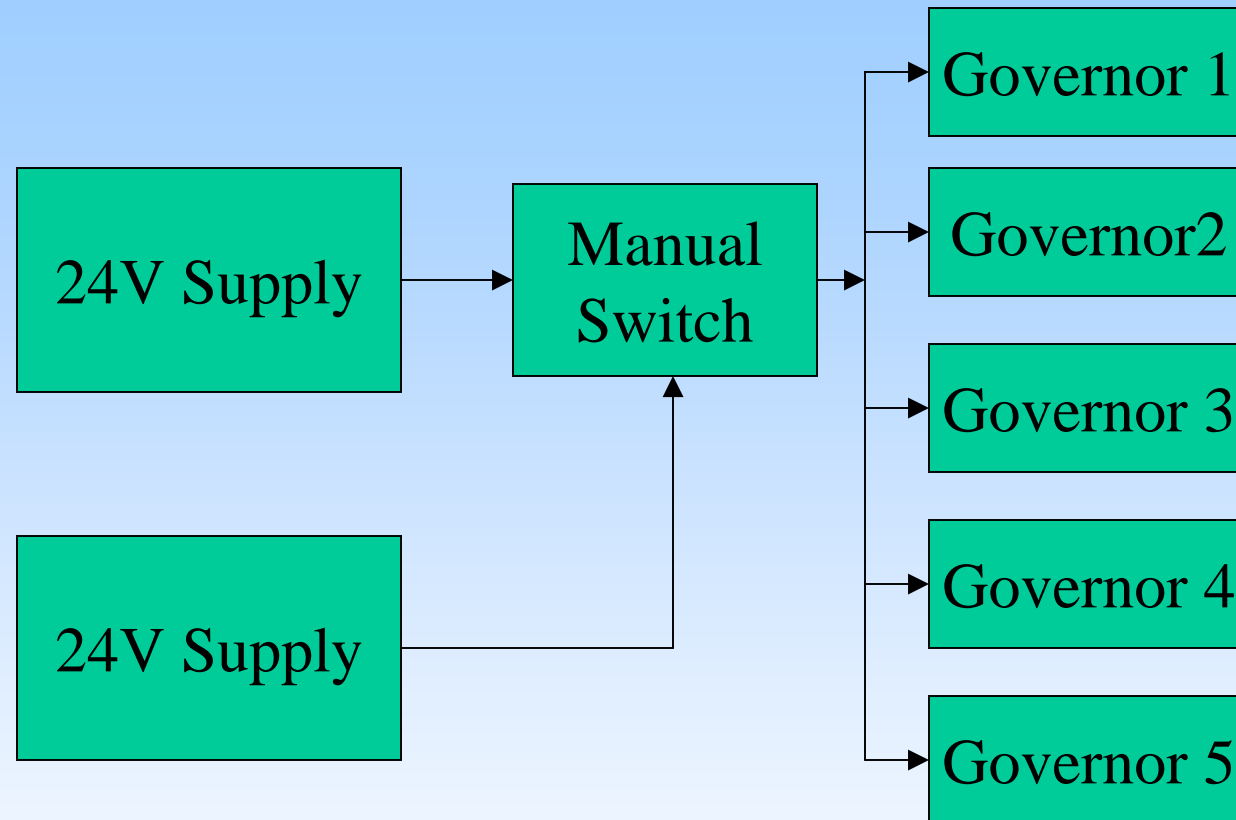
# Example 5 - 'Backed up' Gyros



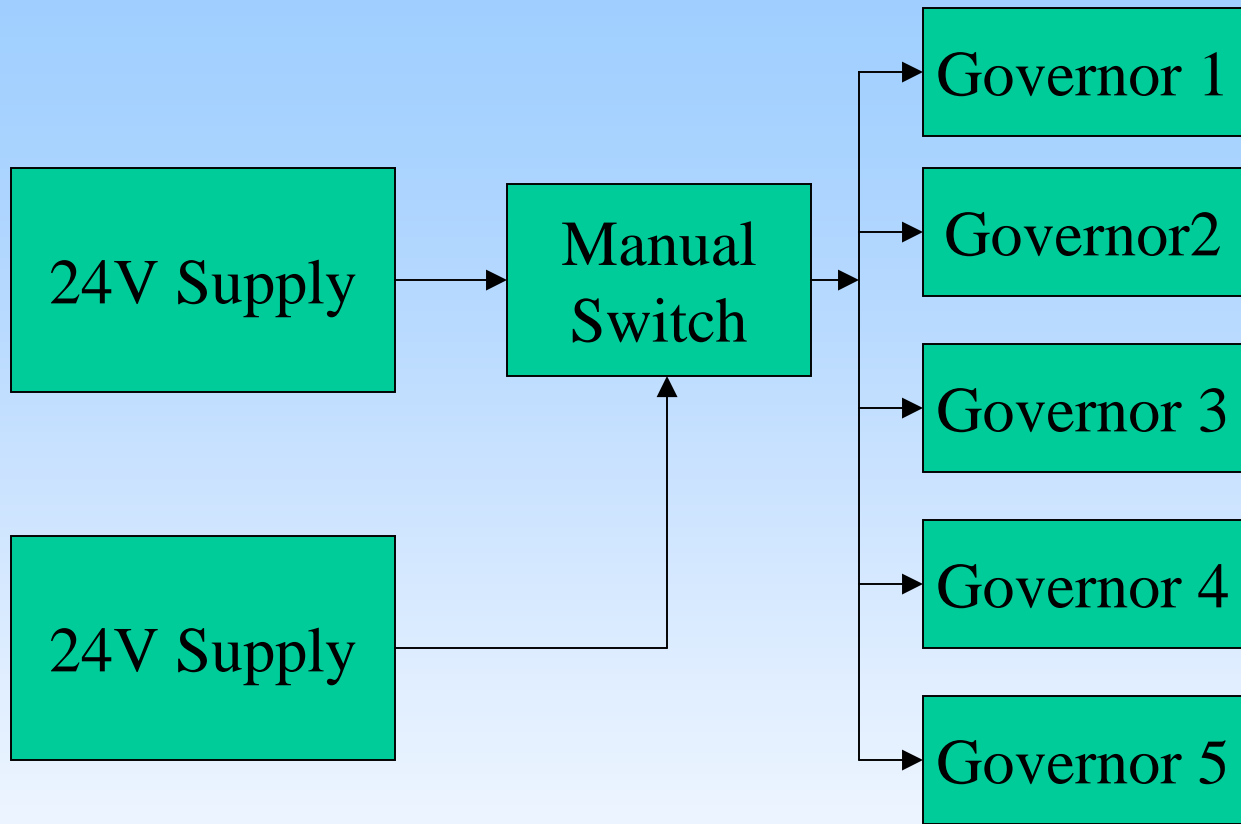
# Example 6 - 'Backed up' 24V



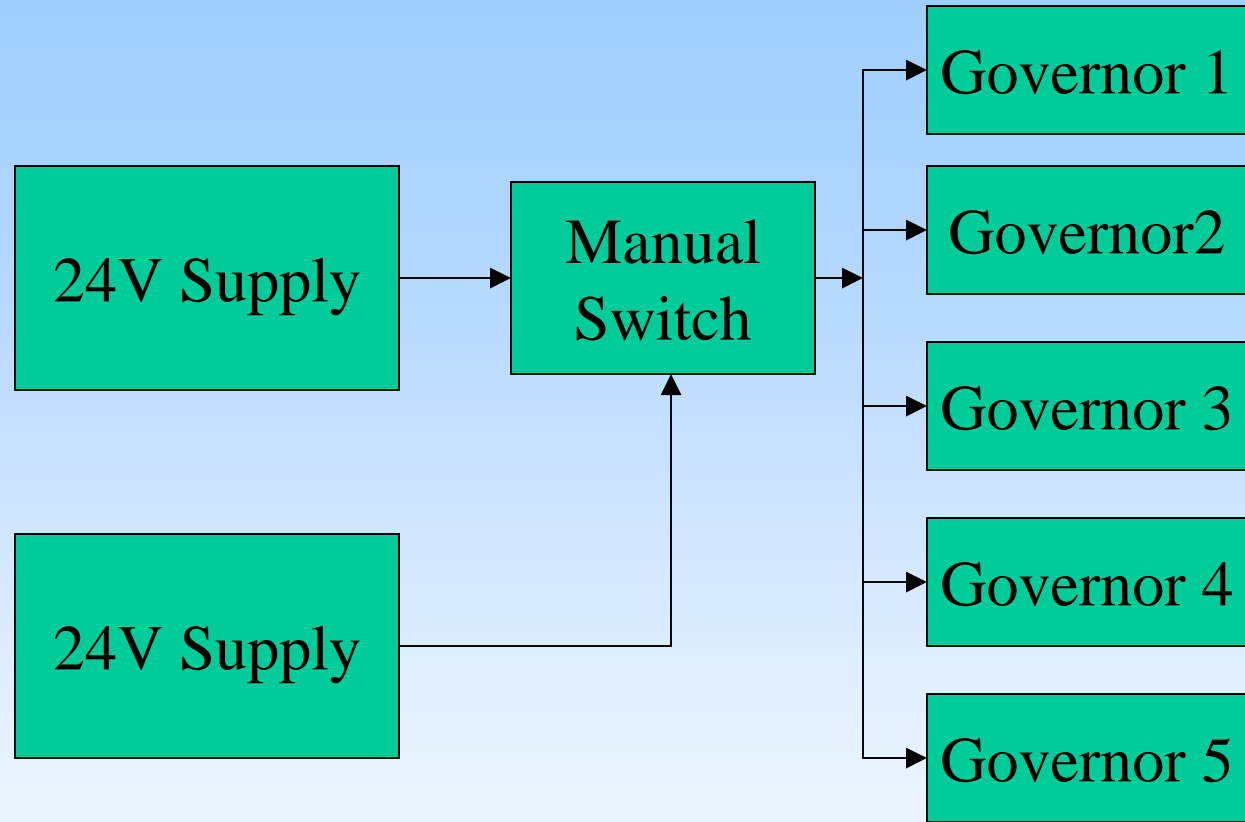
# Example 6 - 'Backed up' 24V



# Example 6 - 'Backed up' 24V

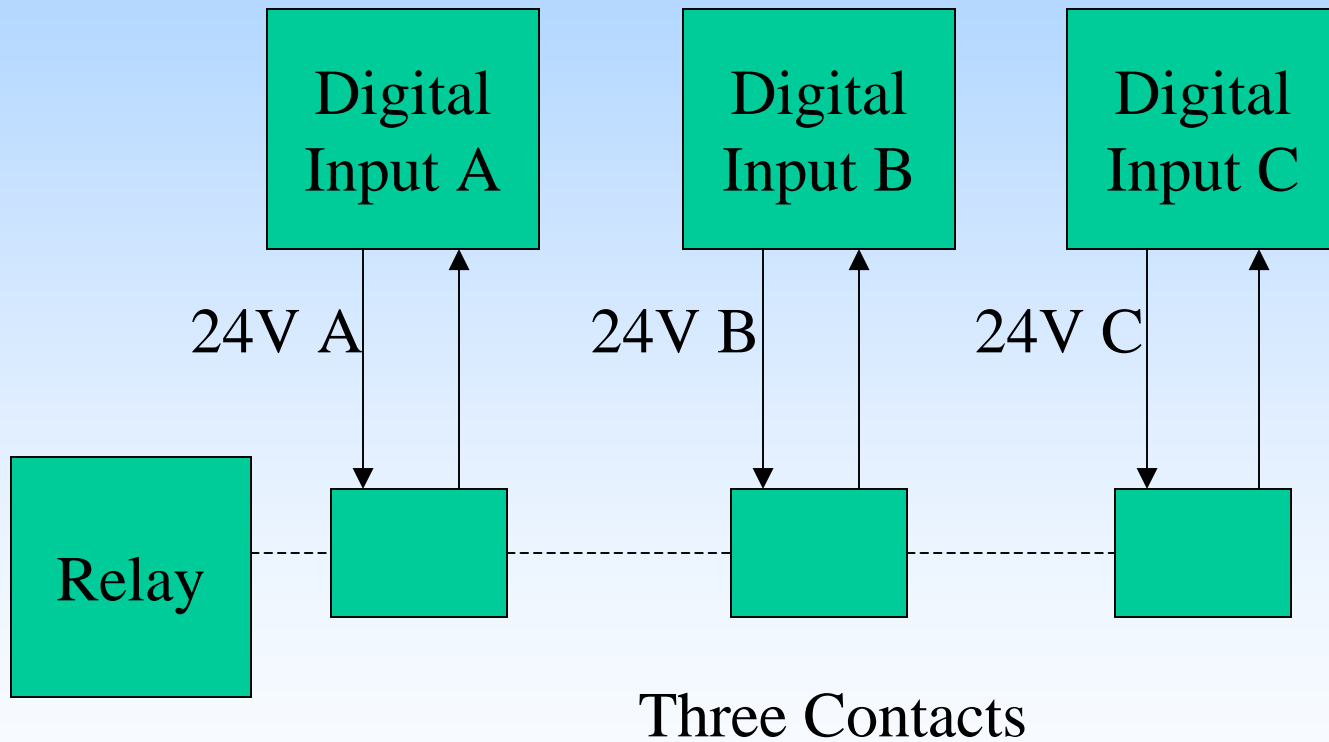


# Example 6 - 'Backed up' 24V

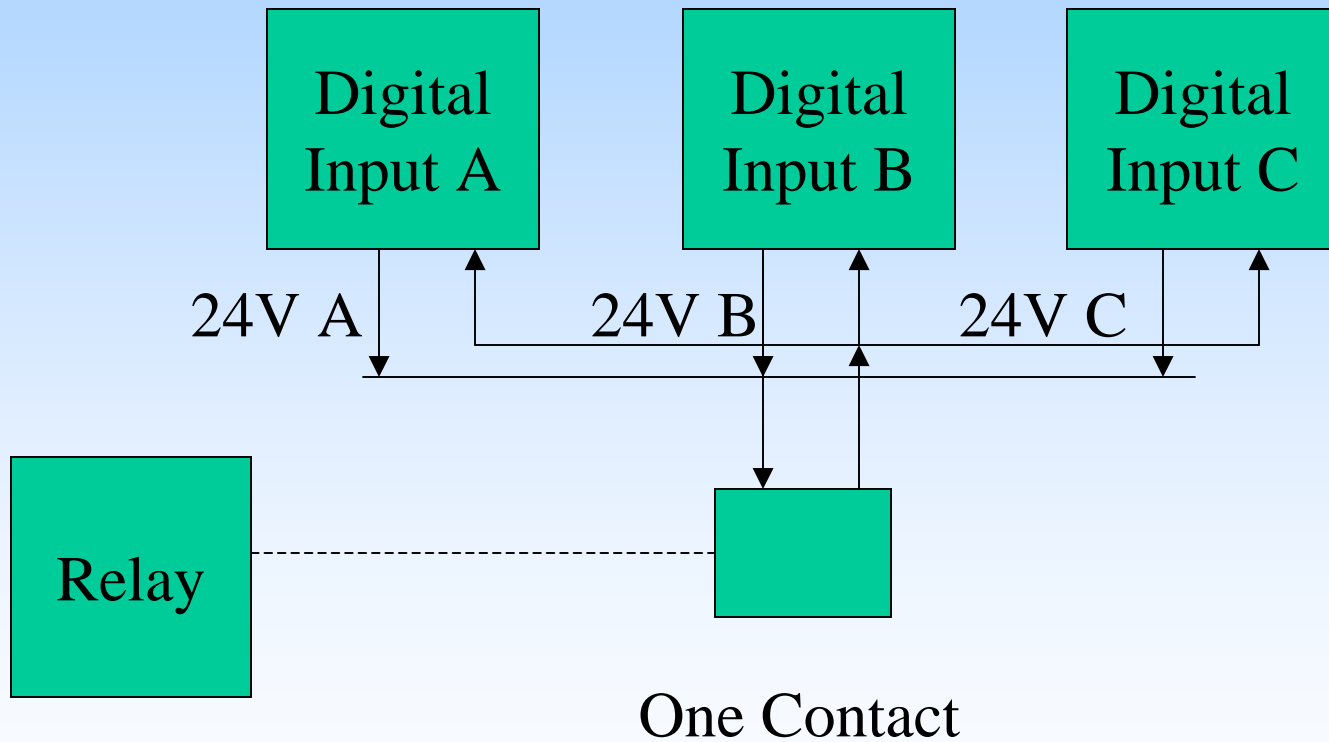


Procedure

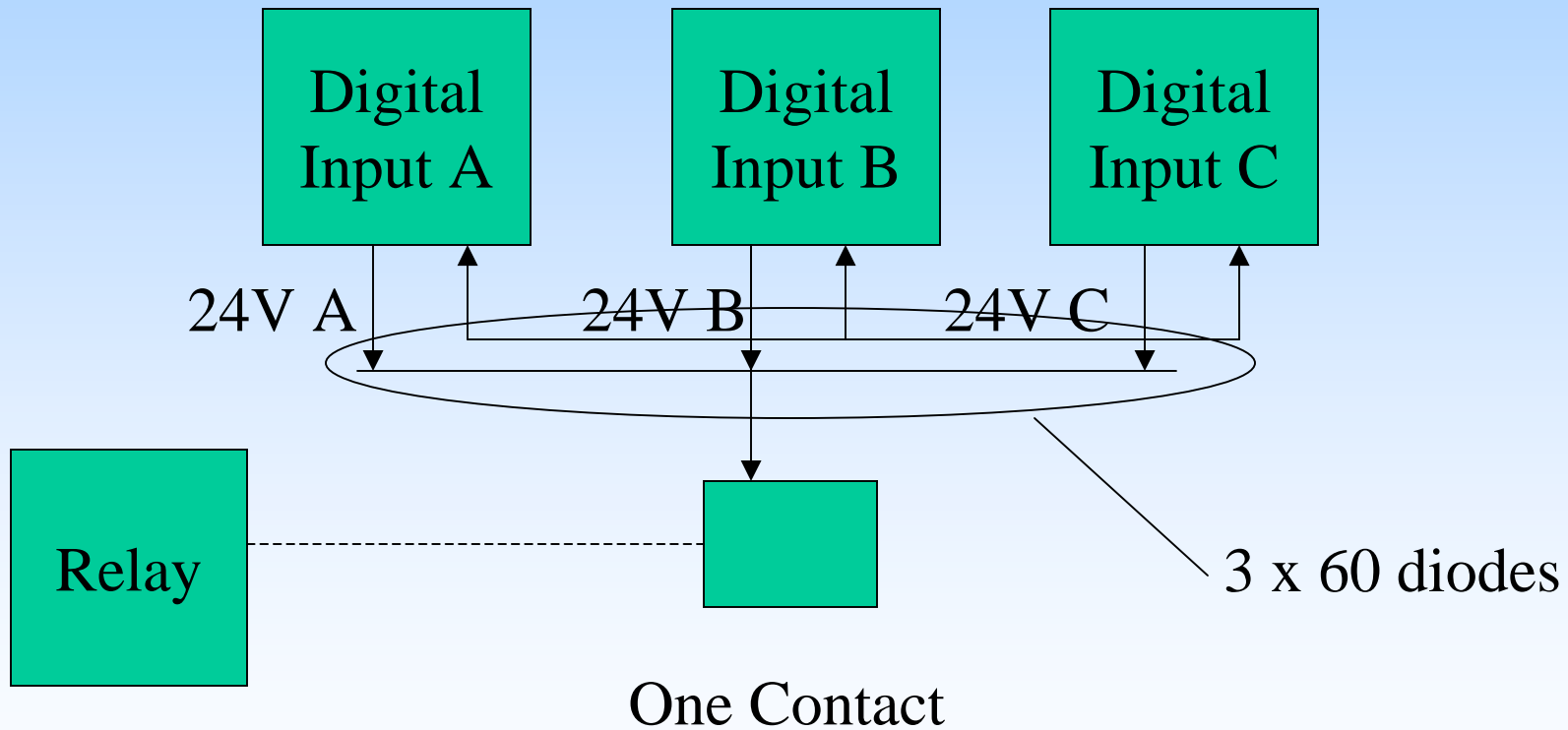
# Example 7 - Diodes Galore



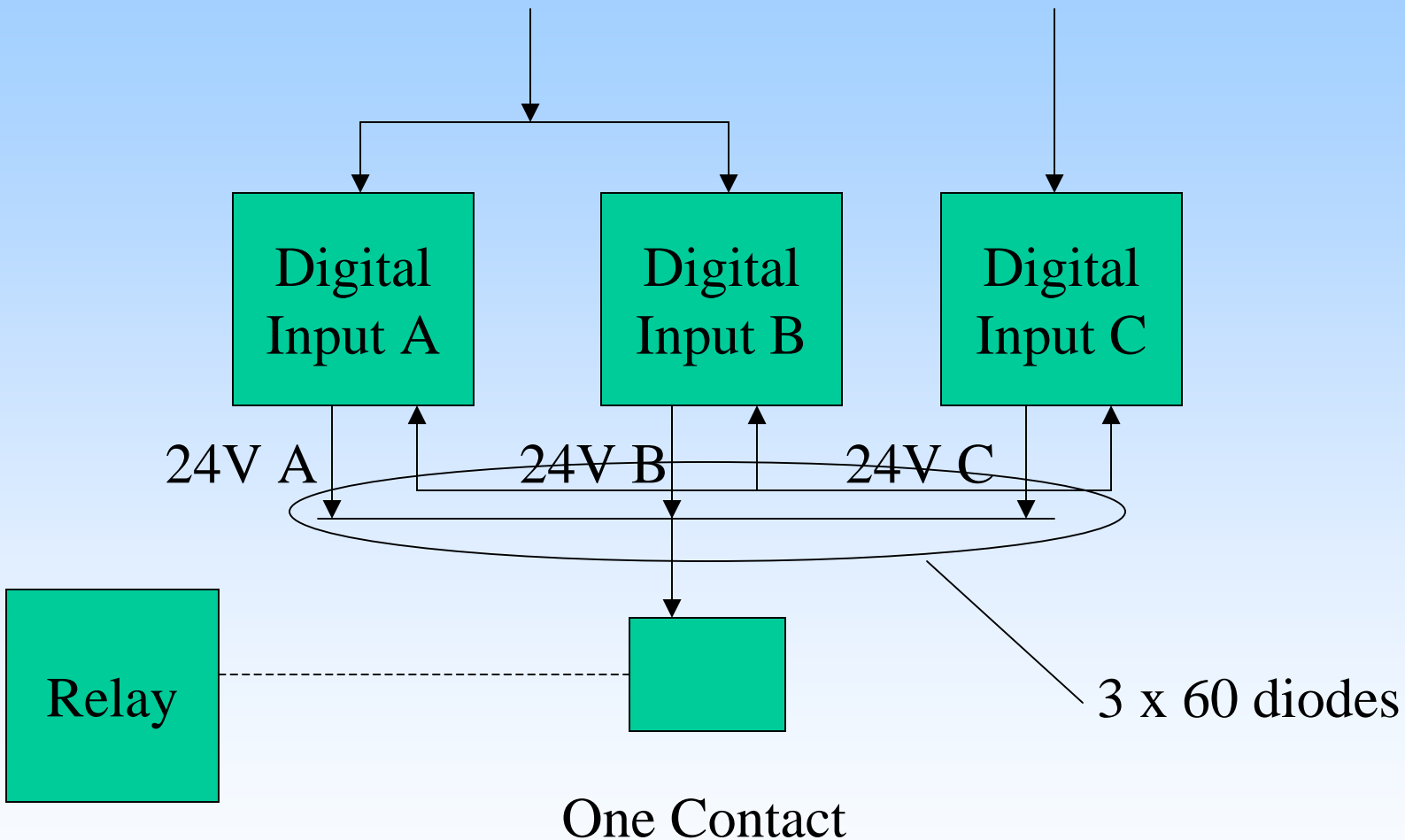
# Example 7 - Diodes Galore



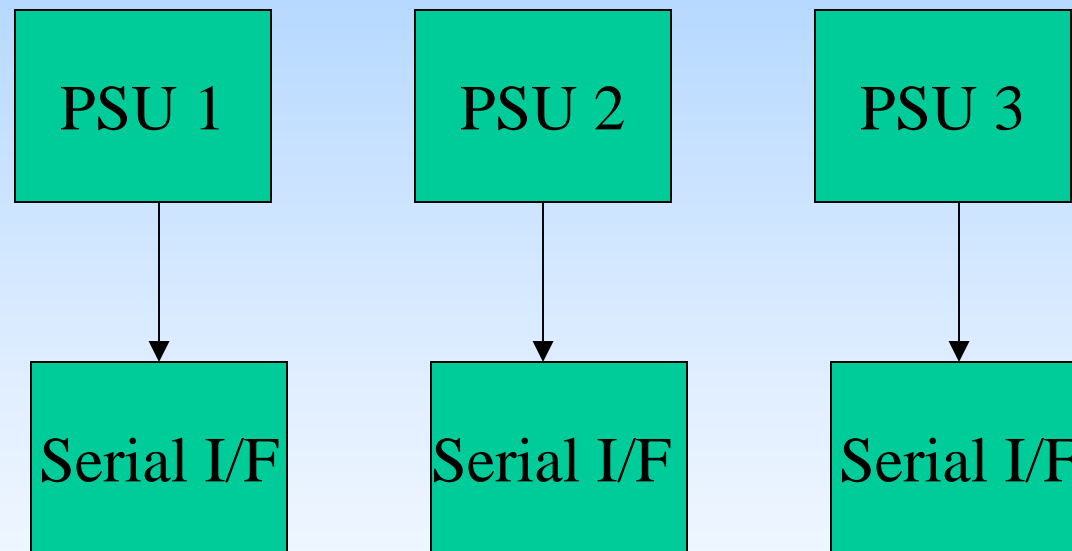
# Example 7 - Diodes Galore



# Example 7 - Diodes Galore

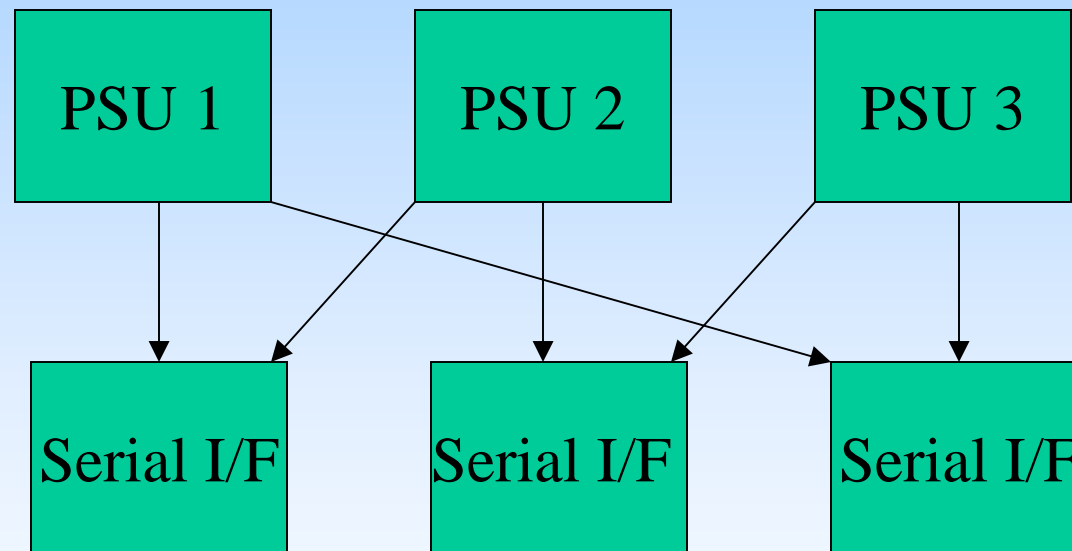


# Example 8 - the heart of a DPCS



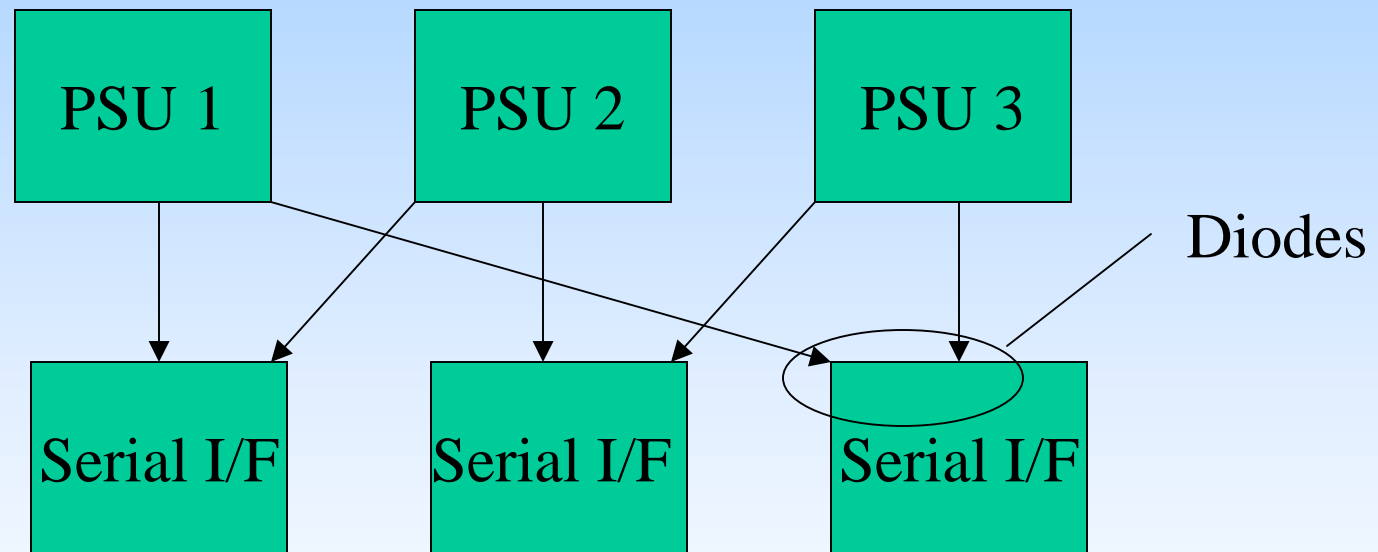
1/3 pos refs and sensors each per UPS

# Example 8 - the heart of a DPCS



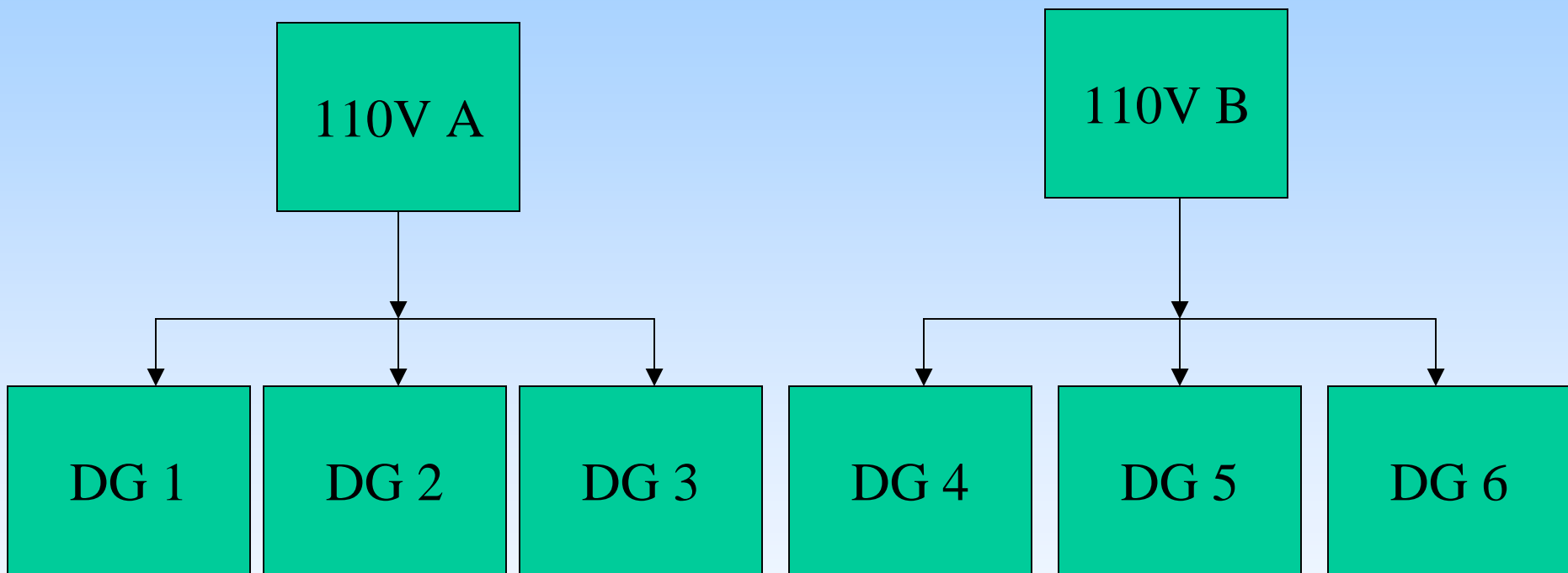
1/3 pos refs and sensors each per UPS

# Example 8 - the heart of a DPCS



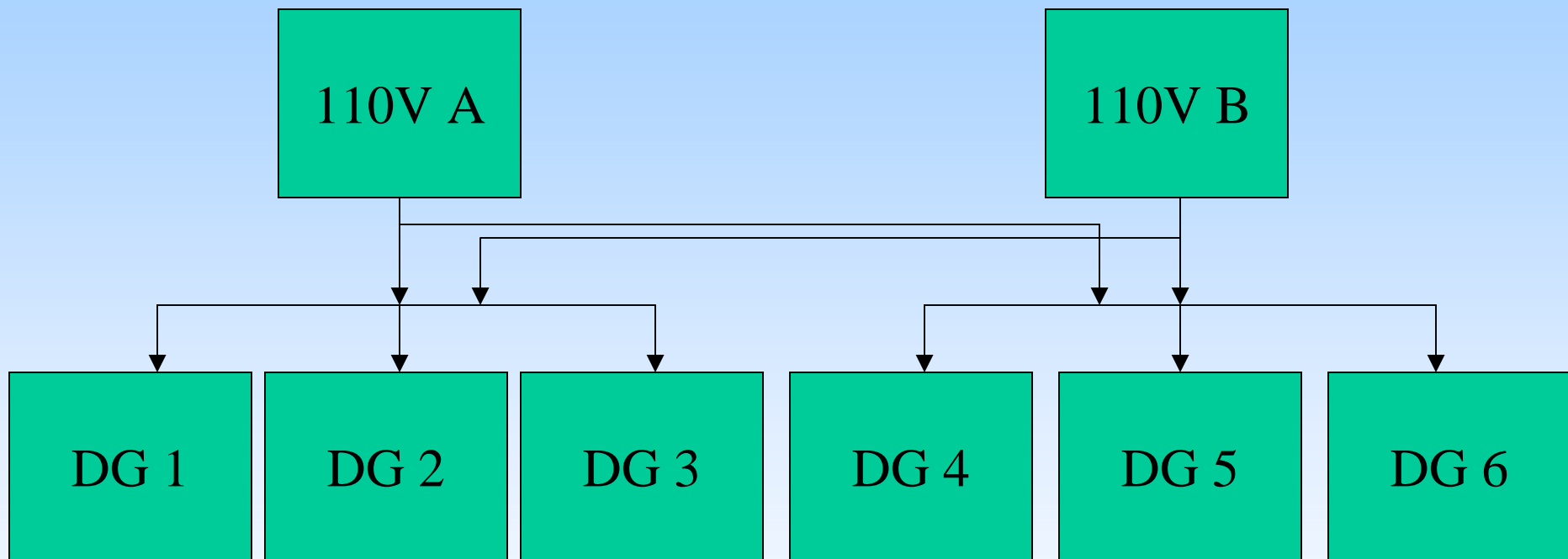
1/3 pos refs and sensors each per UPS

# Example 9 – 110V Diodes



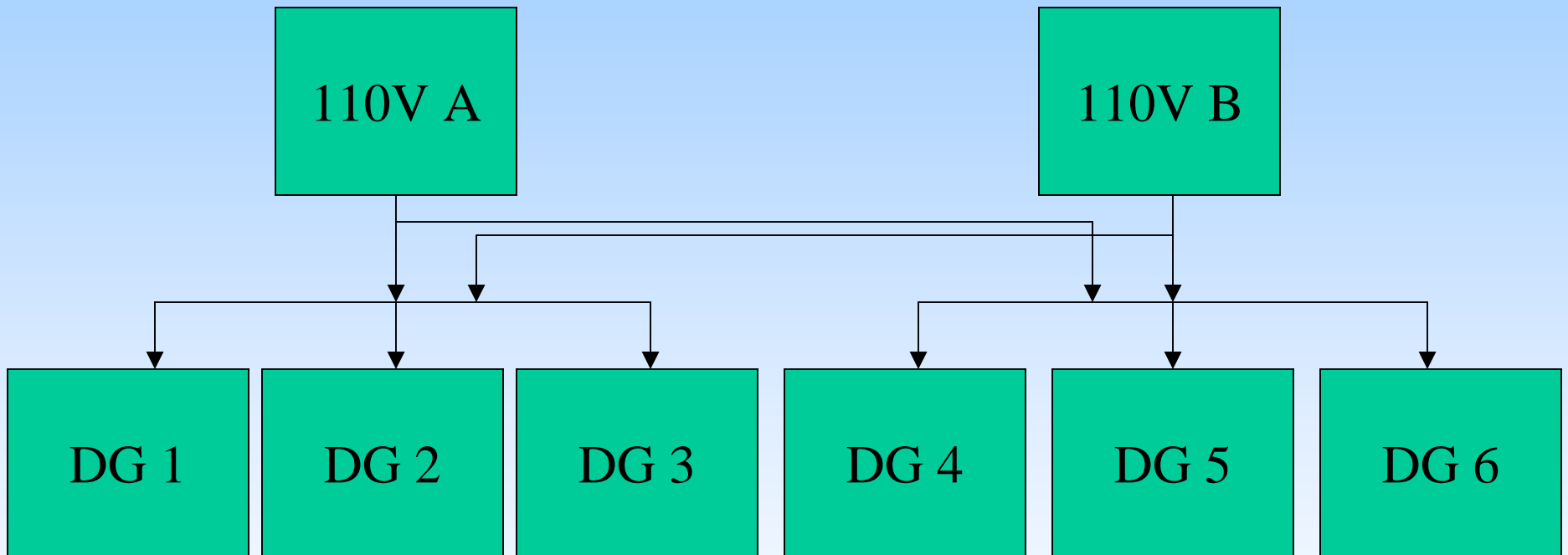
Control and protection supplies

# Example 9 – 110V Diodes



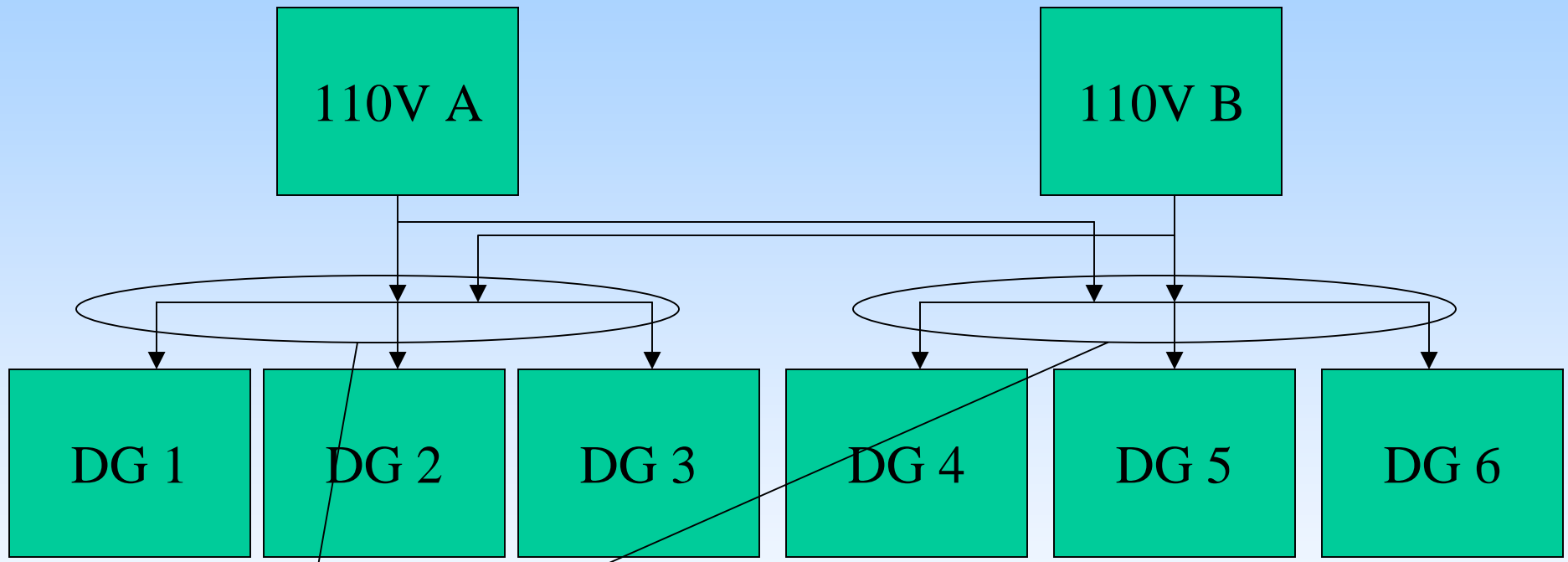
Control and protection supplies

# Example 9 – 110V Diodes



Control and protection supplies

# Example 9 – 110V Diodes



diode and fuse  
for each feed Control and protection supplies

# Example 10

## Example 10

- Emergency recovery system

## Example 10

- Emergency recovery system
- Reconnect thrusters onto healthy side of power distribution

## Example 10

- Emergency recovery system
- Reconnect thrusters onto healthy side of power distribution
- Not worked on 3 annual trials on two identical vessel

## Example 10

- Emergency recovery system
- Reconnect thrusters onto healthy side of power distribution
- Not worked on 3 annual trials on two identical vessel
- No one understands how it works

# Conclusions and Recommendations

# Conclusions and Recommendations

- Owners of class 2 & 3 DP vessels should review their systems for similar ‘improvements’

# Conclusions and Recommendations

- Owners of class 2 & 3 DP vessels should review their systems for similar ‘improvements’
- Of the 10 examples - 5 were site modifications

## Conclusions and Recommendations

- Owners of class 2 & 3 DP vessels should review their systems for similar ‘improvements’
- Of the 10 examples - 5 were site modifications
- No input or peer review from engineering dept. at head office.

## Conclusions and Recommendations

- Owners of class 2 & 3 DP vessels should review their systems for similar ‘improvements’
- Of the 10 examples - 5 were site modifications
- No input or peer review from engineering dept. at head office.
- None subjected to any modification control like a software modification.

## Conclusions and Recommendations

- Owners of class 2 & 3 DP vessels should review their systems for similar ‘improvements’
- Of the 10 examples - 5 were site modifications
- No input or peer review from engineering dept. at head office.
- None subjected to any modification control like a software modification.
- Hardware modification control needs to be in place

# Conclusions and Recommendations

# Conclusions and Recommendations

- All introduced extra complication and made the system more prone to failure and more unreliable.

# Conclusions and Recommendations

- All introduced extra complication and made the system more prone to failure and more unreliable.
- Nearly all introduced the potential for hidden and cascade

## Conclusions and Recommendations

- All introduced extra complication and made the system more prone to failure and more unreliable.
- Nearly all introduced the potential for hidden and cascade
- Nearly all require periodic testing but this does not totally guard against hidden failures.

## Conclusions and Recommendations

- All introduced extra complication and made the system more prone to failure and more unreliable.
- Nearly all introduced the potential for hidden and cascade
- Nearly all require periodic testing but this does not totally guard against hidden failures.
- *Would only know that there were none last time it was tested.*

# Conclusions and Recommendations

# Conclusions and Recommendations

- Configuration errors are introduced.

# Conclusions and Recommendations

- Configuration errors are introduced.
- Systems may no longer be independent

# Conclusions and Recommendations

- Configuration errors are introduced.
- Systems may no longer be independent
- Use of diodes needs to be avoided.

# Conclusions and Recommendations

- Configuration errors are introduced.
- Systems may no longer be independent
- Use of diodes needs to be avoided.
- There are still DP control systems rely on diodes.

# Conclusions and Recommendations

# Conclusions and Recommendations

- Additional complication for fault tolerant only introduces more potential faults

# Conclusions and Recommendations

- Additional complication for fault tolerant only introduces more potential faults
- Not necessarily leave the DP system in class.

# Conclusions and Recommendations

- Additional complication for fault tolerant only introduces more potential faults
- Not necessarily leave the DP system in class.
- KISS –

# Conclusions and Recommendations

- Additional complication for fault tolerant only introduces more potential faults
- Not necessarily leave the DP system in class.
- KISS –
- Albert Einstein's

## Conclusions and Recommendations

- Additional complication for fault tolerant only introduces more potential faults
- Not necessarily leave the DP system in class.
- KISS –
- Albert Einstein's  
**"everything should be made as simple as possible, but no simpler"**

# Conclusions and Recommendations

- Additional complication for fault tolerant only introduces more potential faults
- Not necessarily leave the DP system in class.
- KISS –
- Albert Einstein's  
**"everything should be made as simple as possible, but no simpler"**

# Conclusions and Recommendations

- Additional complication for fault tolerant only introduces more potential faults
- Not necessarily leave the DP system in class.
- KISS –
- Albert Einstein's  
**"everything should be made as simple as possible, but no simpler"**

# FAILURE IS AN OPTION

**Doug Phillips**