



CANDU Safety

#9 - Grouping & Separation

Dr. V.G. Snell
Director
Safety & Licensing



Purpose of Grouping & Separation

- λ protection against events affecting a limited area of the plant
- λ common cause failures:
 - turbine disintegration and resultant missiles
 - fires
 - small aircraft strikes
 - failure of common support system
 - common adverse environment
- λ ensure that functional interconnections between systems do not change effectiveness for accidents



Two Group Design Philosophy

- λ ensure two independent ways to achieve same safety functions:
 - shutdown
 - remove decay heat and/or prevent release of radioactivity
 - monitor the plant
- λ group safety-related systems into two groups
 - Group 1 and Group 2
- λ reactor building is a natural barrier for some common cause events
 - both Group 1 & Group 2 systems are within reactor building



Three Types of Safety-Related Systems

- λ special safety systems
 - shutdown system 1, shutdown system 2, ECC, containment
- λ safety support systems
 - provide electrical power, instrument air & cooling water to special safety systems
- λ safety-related process systems
 - process systems which can mitigate an accident

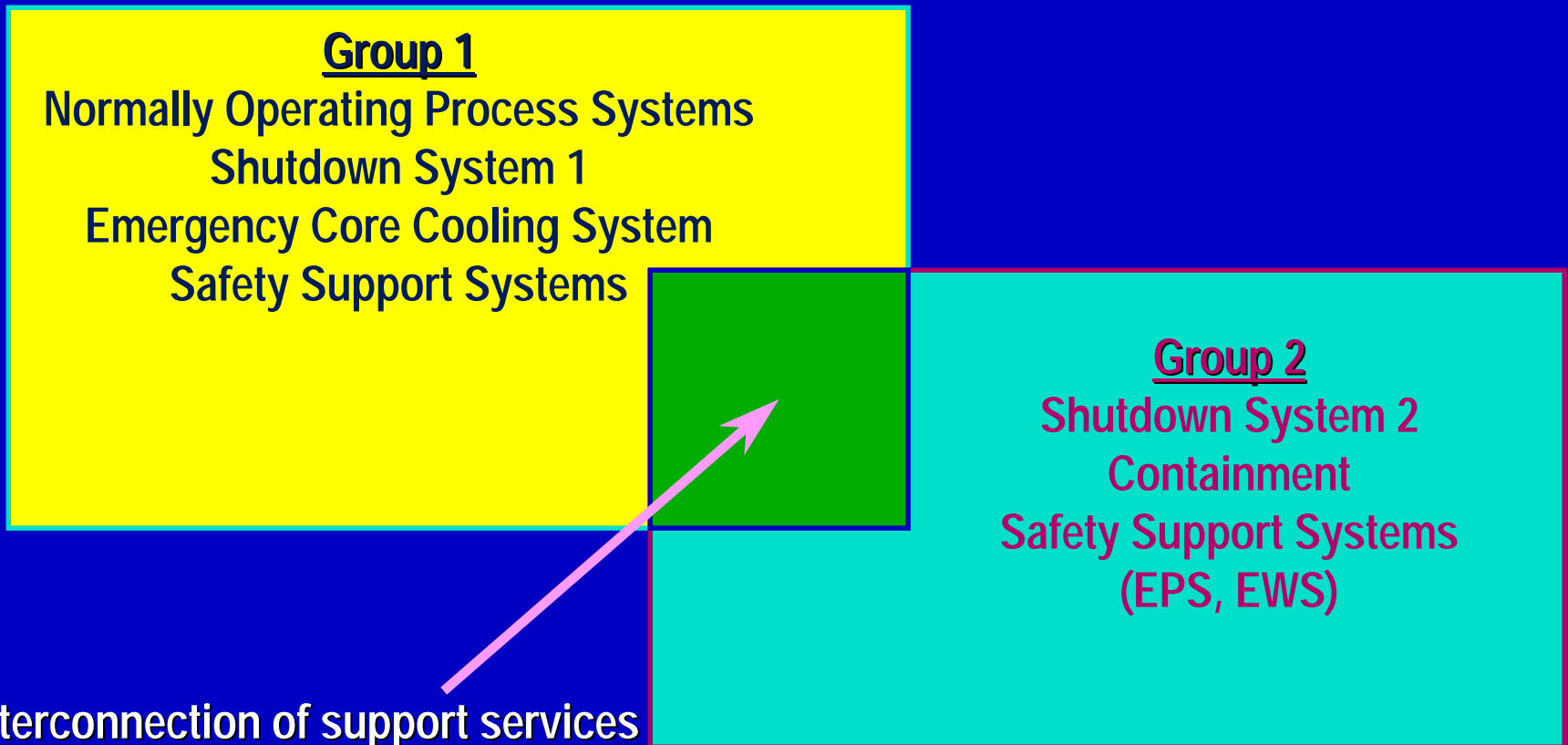


Grouping

- λ each safety-related system assigned to one Group
- λ each Group can independently perform all the safety functions
- λ Group 1
 - power production systems
 - some of the special safety systems
 - safety support systems required by these special safety systems
- λ Group 2
 - the remaining special safety systems
 - safety support systems required by these special safety systems



Systems Within Groups



Interconnection of support services

Group 1 to Group 2 in Normal Operation

Group 2 to Group 1 in accidents

Group 1 to Group 2 in accidents



System Grouping by Safety Function

<i>Safety Function</i>	<i>Group 1 Systems</i>	<i>Group 2 Systems</i>
<i>Shutdown</i>	Reactor Control System Shutdown System 1	Shutdown System 2
<i>Heat Removal From Fuel</i>	Heat Transport System Steam & Feedwater Systems Shutdown Cooling System ECC Moderator	Emergency Water System
<i>Contain Radioactivity</i>	Reactor building air coolers	Containment & containment subsystems
<i>Monitoring & Control</i>	Main Control Centre	Secondary Control Area



Rationale

- λ two shutdown systems are in separate groups so that a single event cannot prevent shutdown
- λ ECC and containment are in separate groups so that a single event cannot damage fuel and allow radioactivity to escape
- λ on CANDU 9, the grouping of containment and ECC has been switched for convenience in cable routing



Safety Support Systems

<i>Safety Support Function</i>	<i>Group 1 Safety Support</i>	<i>Group 2 Safety Support</i>
<i>Electrical power</i>	Class IV Class III diesels Class II Class I	EPS Diesels Class II Class I
<i>Service Water</i>	Raw Service Water Recirculating Service Water	Emergency Water System
<i>Instrument Air</i>	Instrument Air System	Local Air Tanks

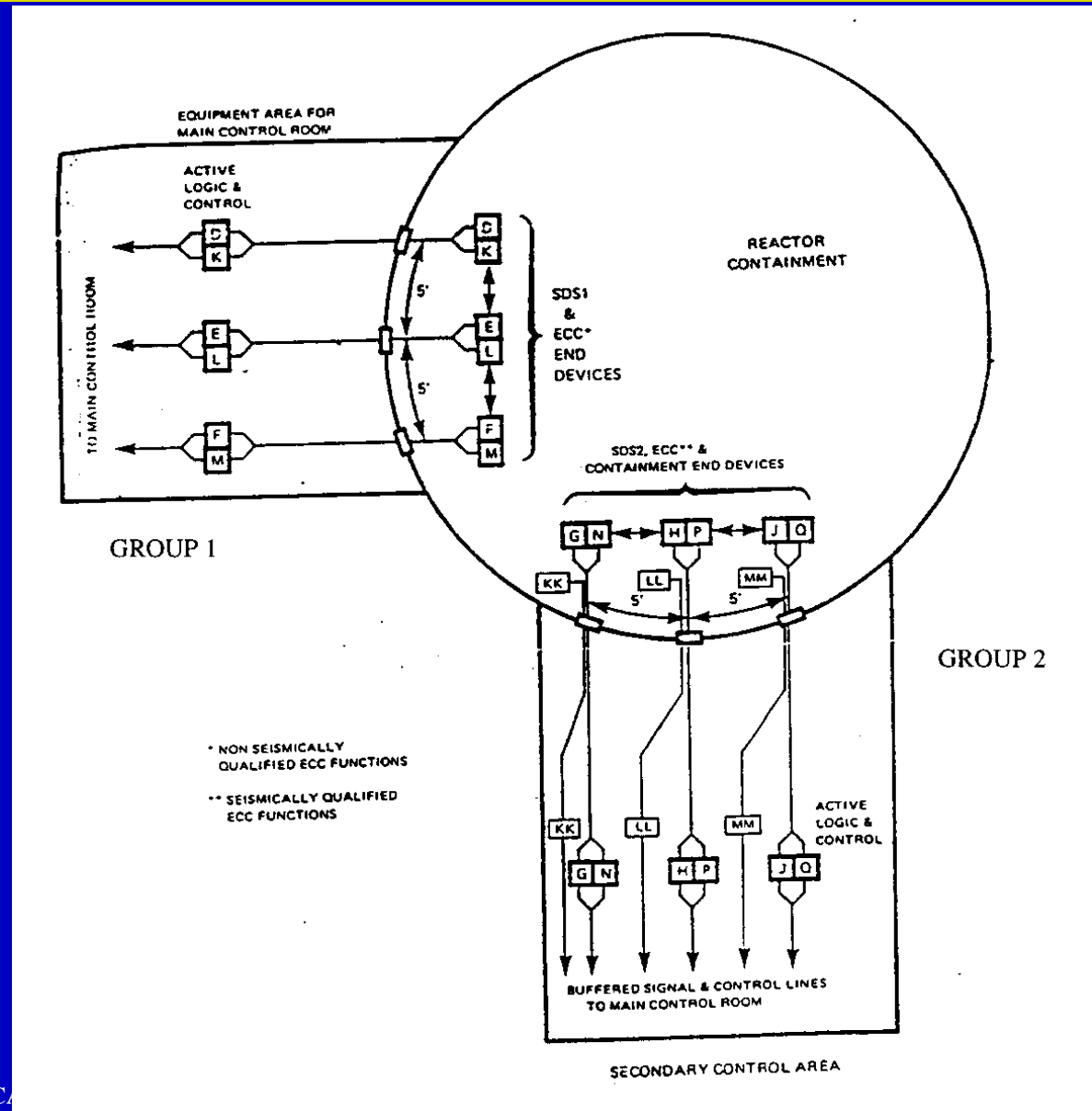


Separation Between Groups

- λ outside reactor building, Groups in different areas of the plant
- λ typically 90 degree separation
- λ separate buildings for Emergency Power System diesels, Emergency Water System
- λ inside reactor building: barriers and physical separation to extent practical
- λ separation barrier or distance assessed to show adequacy
 - fire, missiles, harsh environment
- λ main control room protected from steam line breaks and external events so operators can proceed to SCA; access route protected



Plant Layout





Avoidance of Common Cause Failures

- λ where specified separation cannot be achieved:
 - show no credible hazard in area
 - another Group 2 system outside the area will mitigate
 - system or component protected by barrier
 - system or component is fail safe
 - component designed to withstand hazard
- λ Group 2 systems generally seismically qualified
- λ location above flood levels



Instrumentation Cable Designations

<i>System Group</i>	<i>System Name</i>	<i>Channel Designation</i>		
1	Reactor Regulating System	A	B	C
1	Shutdown System No. 1	D	E	F
1	Emergency Core Cooling System	K	L	M
2	Shutdown System No. 2	G	H	J
2	Containment System	N	P	Q
1	Emergency Core Cooling System (seismically qualified)	KK	LL	MM



Separation Within Groups (Examples)

- λ safety system triplicated instrumentation channels within a group separated by 1.5 metres
- λ power supplies split into "ODD" & "EVEN" to serve redundant components within a Group
- λ "ODD" & "EVEN" cables separated by 1.5 metres
- λ single channels within same Group can share common routing (e.g., A, D, K)
- λ buffering of connections between Main Control Room & SCA
- λ power cables >600 volts must be 0.45m. above instrumentation cables



Isolatable or Buffered Interconnections - 1

- λ Buffered control and instrumentation cables between the Main Control Room and the Secondary Control Area
 - to enable Group 2 equipment to be controlled from the Main Control Room****
- λ Buffered post-accident monitoring and control cables**
- λ Electrical power supply from the grid or from the turbine generator to Group 2 components, where required for reliability**
- λ Cooling water supply from Group 1 to Group 2 components, where Group 1 supplies remain available or can be re-established for long-term reliability**

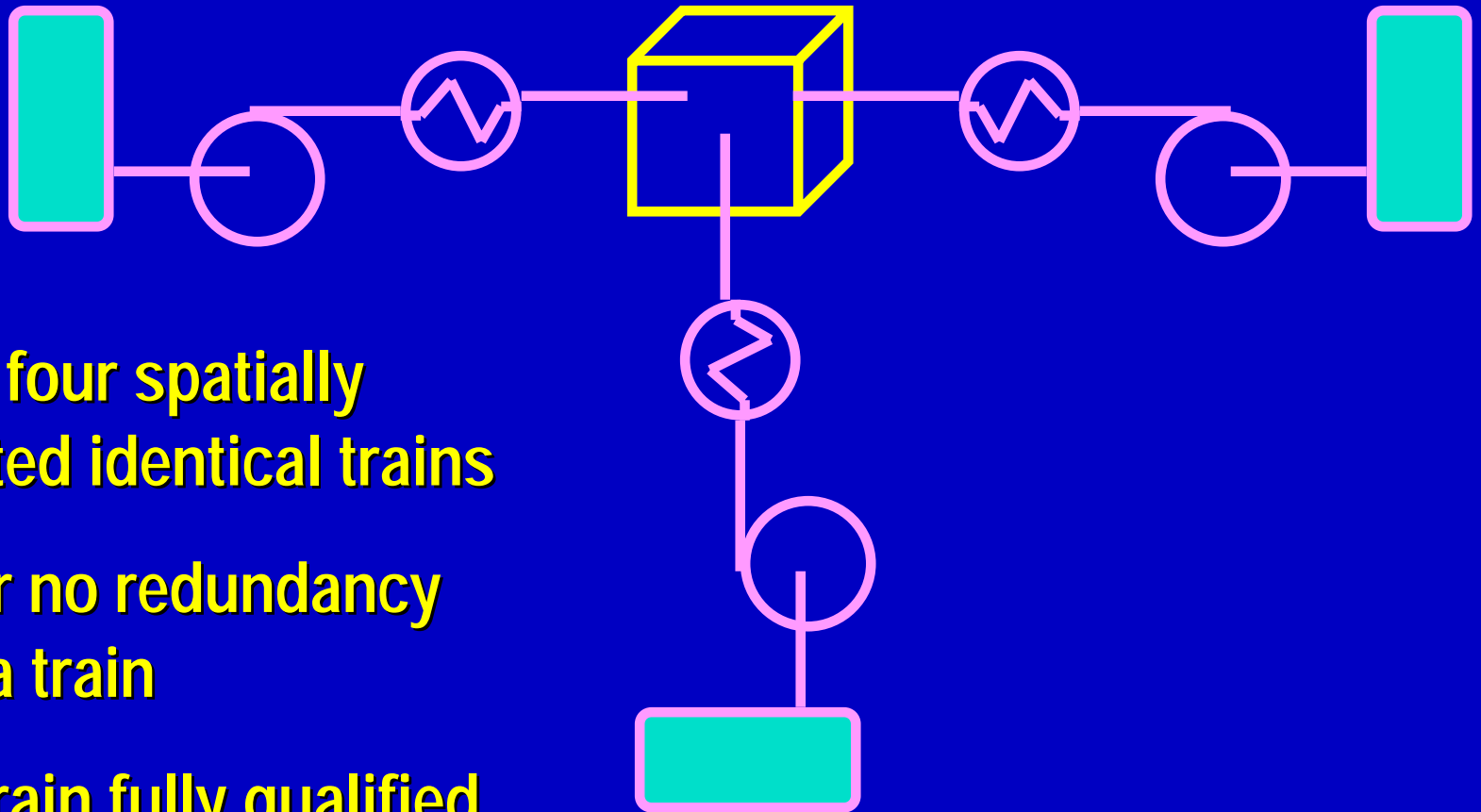


Isolatable or Buffered Interconnections - 2

- λ Compressed air supply from Group 1 for the supply of air storage tanks during normal operation of the plant**
- λ Support services from Group 2 (i.e., EWS, EPS) to Group 1 Special Safety Systems and other safety related components (e.g., supplies to ECC)**
- λ interconnections must ensure that failures cannot propagate from one Group to the other**



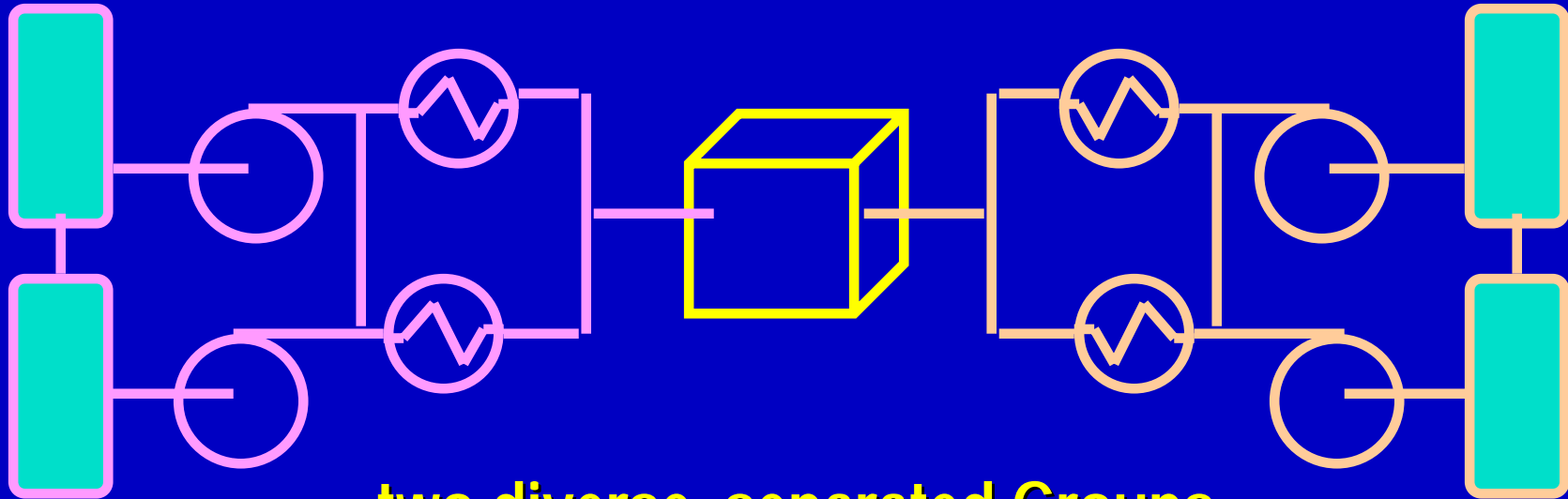
LWR Approach (simplified)



- two to four spatially separated identical trains
- little or no redundancy within a train
- each train fully qualified



CANDU Approach (simplified)



- two diverse, separated Groups
- redundancy within each Group
- qualification determined by safety function



Summary

- λ common cause failures handled by grouping & separating mitigating systems
- λ each group can perform key safety functions
- λ separation protects against common cause failures of both groups
- λ groups have limited cross-connections to increase reliability of mitigation for more frequent events
- λ diversity is more important than redundancy
- λ qualification depends on each specific accident to be mitigated