Process Hazard Analysis (PHA) Study

Death Star – HAZOP Update

REV	DATE	APPROVED	DESCRIPTION OF CHANGE
0	03.04.2020	D.V.	First Issue

Automatically generated by exSILentia version 4.7.0.6991

Table of Contents

1 Scope of Review

1.1 General Information

Project Identification:	DS-1 Orbital Battle Station
Project Name:	Death Star - ReHAZOP
Project Leader:	Tim C
Project Description:	The Death Star is a mobile space station and galactic superweapon. Death Star 1 (DS-1) is 120 kilometers in diameter, and is crewed by a 350,000 military personnel. Designed for massive power-projection capabilities, capable of destroying an entire planet with a 6.2xE32 J/s power output blast from its superlasers

Affiliation: Galactic Empire

Launched: n/a (A long time ago), constructed in space.

Combat vehicles: TIE Fighters

General characteristics

Class: Space Battle Station

Armaments: Superlaser

Defenses: Turbolasers, Laser cannons, Tractor beams, and Ion cannons

Maximum speed: Faster than light speed

Propulsion: Imperial Hyperdrive

Power: Able to destroy a planet with one shot of the superlaser

Width: 120 km (Death Star I)

Other features:

- An equatorial trench divides the Death Star into two hemispheres, each of which issubdivided into 12 bridge-controlled zones for a total of 24 zones. Each zone was similar to a sub-battle station, and has its own food replicators, hangar bays, detention blocks, medical centers, armories, and command centers. (taken from P21, Haynes Imperial Death Star Manual)

- The Death Star is built to defy all planetary defences, and have the ability to destroy an entire world with one devastating stroke. The upper hemisphere houses the superlaser, and all Imperial estimates indicate that a single blast would equal the combined firepower of the entire Imperial fleet. (taken from P21, Haynes Imperial Death Star Manual).

- 35 kilometers in diameter, the superlaser focus dish is the Death Star's most prominent feature. (taken from P22, Haynes Imperial Death Star Manual)

- When the first Death Star's construction was finished, it was the single largest

object ever built. (taken from P21, Haynes Imperial Death Star Manual)

- The Death Star's armament features 1 superlaser, 15,000 Taim & Bak D6 turbolaser batteries, 2,500 Borstel Galactic Defense SB-920 laser cannons, 2,500 Borstel MS-1 ion cannons, 768 Phylon tractor-beam emplacements and 11,000 combat vehicles. (taken from P23, Haynes Imperial Death Star Manual)

- The Death Star personnel comprises 342,953 military (285,675 operational staff and 57,278 gunners) and 843,342 passengers. It can also carry over one million kilotons of cargo and 3 years' worth of consumables." (taken from P23, Haynes Imperial Death Star Manual)

Operational Experience 5-Years:

- 14 planets destroyed

- 22 Rebel Alliance attacks repulsed

- Issues / Lessons Learned: Two cases of port overheating. Root Cause Analysis Failure 1: Light sabre blocking port. Root Cause Analysis Failure 2: Operator error

- Current alarm historian status: Warning light on City Sprawl North 7: A68 Ray Shield Generator causing nuisance alarm. Trip override in place, final repair pending budget approval

- Operator 1 Feedback: Good experience, no issues

- Operator 2 Feedback: Food poisoning due to contaminated cantine food, affecting Operators ability to react to alarms

Record from previous PHA ('What the Death Star can tell us about Ergonomics Methods', Guy Walker et. al) denoted by : PHA

New HAZOP record denoted by: HAZOP-Update

Business (B) and Environmental (E) risk excluded from risk ranking. Only Safety (S) considered.

1.2 Participants

The PHA team was comprised of the following participants.

Table 1 HAZOP Participants

NAME	ROLE
Raith Sienar	DENG - Design
Bevel Lemelisk	DENG - Design
Galen Erso	DENG - Design
Darth Vader	LORD - Lord
Tarkin	GM - Grand Moff
Krennic	DIR - Director

NAME	ROLE
Arnfried L	PENG - Process
Jason S	ASTRO - Astrophysicist
Theo S	OS - Operations Supervisor
Muriel B	SCRB - Scribe
Tim C	LDR - Leader

1.3 Sessions

The following sessions were recorded during the PHA.

Table 2 HAZOP Sessions

SESSION NAME	DATE		NODES
	STARTED	ENDED	
HAZOP - Detailed Design Phase	A long time ago ...		1
HAZOP Update	27.03.2020	27.03.2020	1

1.4 Unit / Node List

The following Units and Nodes were identified during the PHA.

1: DS-1 Orbital Battle Station

Unit	1: DS-1 Orbital Battle Station
Nodes	1: Thermal Exhaust Port - Expel excess energy (Task Step 2.1.1.5)

1.5 Process Descriptions

This section lists the Process Description for each Unit.

1.5.1 1: Thermal Exhaust Port

A thermal exhaust port is an outlet for dissipating the excess heat produced by the large energy reactors used on board starships and space stations or in certain ground-based structures. These ports draw excess heat energy away from the reactors and other equipment in a structure and expell it into space or the atmosphere to prevent damage to systems or injury to the crew from heat build-up.

Small thermal exhaust ports (2m diameter) scattered over the Death Star's surface open upon shafts leading directly to the main reactor.

Note:

- As-built drawings suggest port may be ca. 50m wide

- Port works by releasing radiation via a 60km long tube from the reactor core area (estimated 1300K) to space (2.7K space black body), no convection (no cooling medium medium). Core radiates isotropically, radiation scatters along 60km exhaust port and and heats port wall metal surface. Port wall transfers heat by conduction to heat sink at surface. Surface heat sink has a capacity control mechanism. There is a shut-off mechanism that allows operators to close-off individual ports.

2 Reference Documents

2.1 Documents Used for this Study

The following reference documents support the Death Star - ReHAZOP.

Table 3 Death Star - ReHAZOP Reference Documents

No.	DOCUMENT NUMBER	TITLE	REV.
1	IEC 61508	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems	2010
2	IEC 61511	Functional safety: Safety Instrumented Systems for the Process Industry Sector	2017
3	ANSI/ISA 84.00.01	Functional safety: Safety Instrumented Systems for the Process Industry Sector	2004
4	IEC 62443	Industrial Communication Networks-Network and System Security	2009
5		What the Death Star can tell us about Ergonomics Methods, Guy Walker et. al.	2016
6		Death Star Technical Companion © West End Games	1991
7		Imperial Death Star - Owner's Workshop Manual © Haynes	2013

2.2 Applicable Regulatory Standards

The following documents represent the regulatory standards that apply to the Death Star - ReHAZOP.

Table 4 Death Star - ReHAZOP Applicable Regulatory Standards

N.A.

3 Study Methods and Results

3.1 PHA Objectives

The primary objective of the PHA study is to identify the risks of potential safety and environmental hazards, as well as major operability problems. This is done for each node by identifying and documenting initiating events, consequences, and associated safeguards. When the existing safeguards were found to be insufficient based upon the as found risk, the multi-disciplinary PHA team proposed recommendations to reduce the risk and/or enhance operability in order to satisfy risk criteria established at the outset of the review.

3.2 PHA Methods Utilized

The HAZOP (HAZard & OPerability study) methodology was used as the primary PHA technique. HAZOP is a qualitative risk assessment tool used to identify chemical, physical, or changing conditions, which have the potential for causing damage to human life, the environment, or property. A summary of the method is included below:

- Select Node
- Select Deviation (‚procedural' guidewords)
- Identify & Record Causes
- Identify & Record Qualitative Cause Likelihood
- Identify & Record Consequences (without safeguards)
- Determine & Record Qualitative Severity of Consequences
- Identify & Record Safeguards Applicable to Cause or Consequence
- Determine & Record Qualitative Likelihood (with existing safeguards)
- Determine if Tolerable Risk. If not make recommendation(s)

3.3 Risk Ranking

The risk ranking matrix used during the Re-HAZOP is shown below, followed by consequence severity and likelihood definitions.

Consequence Severity	Likelihood					
	1	2	3	4	5	6
6	10	16	20	25	30	36
5	5	10	16	20	25	30
4	4	9	14	16	20	25
3	3	4	9	14	16	20
2	2	2	2	3	8	14
1	1	1	1	1	1	1

Level	Severity		
	B	E	S

Level	Severity		
	B	E	S
1	Negligible impact	Negligible impact	Negligible impact
2	$50,000 - $500,000	Temporary release and cleanup within weeks	Recordable injury
3	$500,000 - $5 million	Temporary damage to the facility and cleanup within months	Lost time injury
4	$5 million - $50 million	Temporary damage to the facility and cleanup within years	Irreversible injury (e.g. blindness, loss of limb, etc.) or single on site fatality
5	$50 million - $250 million	Temporary damage to the facility and cleanup greater than a decade	On-site fatalities
6	> $250 million	Permanent damage to environment rendering land unusable	Off-site fatalities

Level	Likelihood
	L
1	< 10-5 per year
2	10-4 to 10-5 per year
3	10-3 to 10-4 per year
4	10-2 to 10-3 per year
5	10-1 to 10-2 per year
6	> 10-1 per year

3.4 Recommendations and Worksheets

The list of recommendations made during the HAZOP review is included in Appendix A. The HAZOP worksheets are included in Appendix B.

3.5 HAZOP Revalidation

HAZOP revalidation shall be done by updating and revalidating the previous HAZOP or by conducting a new HAZOP (redo) or a combination of the two approaches:

1. Update and revalidate
   a) Modify /supplement previous HAZOP to address changes and confirm that the previous HAZOP accurately reflects the hazards of the process and that adequate controls are in place to manage these hazards.
   b) This may include upgrading the previous HAZOP for items that should have been addressed as part of the previous HAZOP.
2. Redo: Perform a completely new HAZOP as if it were the initial HAZOP.
   a) If significant changes have taken place, a new HAZOP (redo) should be done.

b) If there have not been significant changes or there is confidence that changes have been subject to an effective MOC process, it may be sufficient to review the old study, the changes documented in MOC, to update and revalidate the HAZOP.

Following questions shall be reviewed to determine if a full new HAZOP should be conducted:

- Did the previous HAZOP use methodology consistent with accepted Risk Management?
- Did the previous HAZOP report record the study in full such that the hazards can be identified, even if no recommendations were made?
- Relevant to management of change: have potential hazards been assessed, updates made to the last HAZOP as appropriate, and changes to P&IDs made as appropriate?
- Have potential lessons learned from previous incidents and near misses since the last HAZOP been considered?

If the answer is “No” to any of the questions, the HAZOP shall be redone rather than revalidated.

If the decision is taken to revalidate, a review of the previous HAZOP log sheets should consider:

- Refreshing knowledge and understanding of hazards and safeguards and verifying that they are still valid.
- Checking for additional hazards not identified in the previous HAZOP.
- Any change in knowledge or circumstances that might affect the conclusions previously reached regarding the adequacy of the existing safeguards.
- Combining any major modification HAZOPs or change management HAZOPs into the main HAZOP of the unit or facility.

In regard to previous Recommendations:

- Does a system exist for effective and timely closeout of all PHA/HAZOP recommendations?
- Does the system include means of verifying that the recommendation was completed or dismissed? If so, how?
- If a recommendation was rejected, is there sound evidence as to why? Does the hazard still exist?
- Are there any rejected recommendations that the revalidation team believes should not have been, and wants to reissue?
- Did the action taken based on the recommendation require any further safety review? Was it done?

Review the effect of revisions:

- Overview of changes made since the last HAZOP from the perspective of the system as a whole, versus the individual changes.
- Is there a system for MOC? Does the system include identifying the need for a HAZOP?
- Were there any revisions that required engineered changes? If so, was a HAZOP completed for the revision?
- Were there any changes to an alarm or safety system? If so, was a HAZOP required and completed if necessary?
- Did any of the changes require modifying the operating conditions outside the operating range? If so, was a HAZOP or safety review conducted?
- Did any of the change require a modification to the chemistry of the process? Did the change(s) require modification to the timing or sequencing of the operations? If so, was a HAZOP completed?
- Did any of the changes require modifications to the maintenance procedures or schedule? Does the change affect safety or the environment?

- Have process conditions or fluid compositions changed gradually over time without an MOC or safety review being performed?
- Change in staffing level
- Operator experience
- Changes to safeguards
- Changes to equipment reliability
- Changes to safe or operating limits

Review of Previous incidents:

- Were there any incidents or near misses since the last HAZOP? If so, was there a thorough investigation, and was the pertinent information shared with those involved in operating and maintaining the process?
- Were there any incidents from outside the facility (other BP facilities or industry) from which learnings could be applied to the process undergoing HAZOP revalidation?
- Did any changes take place as a result of the incident investigation? If so, was the MOC procedure followed? Was a HAZOP completed if necessary?

PHA quality:

- Are there any known causes of process incidents that were not adequately covered in the baseline PHAs? Have all causes been considered?
- Are there any engineering or administrative controls and their relationships that were not fully discussed in the baseline study? Are there any consequences that were not fully developed in the baseline?
- Were safeguards valid and fully documented?
- Gaps in PHA documentation
- Equipment previously not reviewed

4 Abbreviations and Definitions

4.1 Symbols and Acronyms

BPCS	Basic Process Control System
CCF	Common Cause Failure
CFSE	Certified Functional Safety Expert
CMF	Common Mode Failure
CM	Conditional Modifier
EC	Enabling Condition
E/E/PE	Electrical/Electronic/Programmable Electronic
EMC	Electro-Magnetic Compatibility
ESD	Emergency Shutdown
FAT	Factory Acceptance Testing
FSM	Functional Safety Management
HAZOP	Hazard and Operability Study
IE	Initiating Event
IEC	International Electrotechnical Commission
IPL	Independent Protection Layer
LOPA	Layer of Protection Analysis
MOC	Management of Change
PHA	Process Hazard Analysis
QRA	Quantitative Risk Assessment
RRF	Risk Reduction Factor
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System
SLC	Safety Life Cycle
SOP	Standard Operating Procedure
SRS	Safety Requirements Specification
SVA	Security Vulnerability Assessment

4.2 Definitions

Not used.

5 Disclaimer, Assumptions

5.1 Disclaimer

The user of the PHAx™ software is responsible for verification of all results obtained and their applicability to any particular situation. Calculations are performed per guidelines in applicable international standards. exida.com L.L.C. accepts no responsibility for the correctness of the regulations or standards on which the tool is based. In particular, exida.com L.L.C. accepts no liability for decisions based on the results of this software. The exida.com L.L.C. guarantee is restricted to the correction of errors or deficiencies within a reasonable period when such errors or deficiencies are brought to our attention in writing. exida.com L.L.C. accepts no responsibility for adjustments made to this automatically generated report made by the user.

5.2 Assumptions PHAx™

This PHAx™ (Process Hazard Analysis) HAZOP Report is generated based on information provided by the user. PHAx™ comes with a set of standard deviation options for various elements, but it is up to the user to verify that the available options are applicable and sufficient for the specific plant application and environment.

Appendix A Death Star - ReHAZOP Recommendations

This appendix lists the recommendations provided during the Death Star - ReHAZOP.

Table 5 Death Star - ReHAZOP Recommendations

RECOMMENDATION	ASSIGNED TO	WORKSHEET PLACES USED
1: More sensors on exhaust and source of radiation. HAZOP Update: Existing sensors generate alarm, requiring Operator Action (manually close down port)	Galen Erso	1.1.1
2: Blow up more planets to test function. More test firing. HAZOP Update: 14 planets have been destroyed in 5 years operation. Check operation records to see if large planets have been destroyed (= high load on ports)	Krennic	1.1.1 1.2.1
3: Learn lessons/data from smaller guns on star destroyer. HAZOP Update: 5 years operational experience does not indicate any issue with port dimensions	Krennic	1.1.1
4: Make port bigger to aid flow. HAZOP Update: Retrofit not possible. Design calculations confirm that there is sufficient heat rejection capacity when all ports are in operation	Galen Erso	1.1.1
5: Control of thermal exhaust. HAZOP Update: Redundant ports are available (=ISD, included under non-instrumented safeguards), surface heat sink control mechanism implemented	Galen Erso	1.3.1
6: Cooling/extractor fans. HAZOP Update: does not work in a vacuum	Galen Erso	1.3.1
7: Put a grate over the port. HAZOP Update: Review why grates have not been implemented. It is also noted that the port external opening could be potentially completely blocked off, as this does not significantly impact heat radiation capacity (main heat rejection is via surface heat sink)	Tarkin	1.3.1
8: Re-route flows to other exhaust ports. HAZOP Update: Redundant ports are available (=ISD, included under non-instrumented safeguards), radiation from the core is distributed evenly to all exhaust ports	Galen Erso	1.3.1
9: Designated cool down period (procedural change). HAZOP Update: Confirm if cooldown period is implemented in operational procedures and / or consider to incorporate timer interlock that limits laser restart frequency	Krennic	1.5.1
10: Back up for life support. HAZOP Update: Action still open	Krennic	1.5.1
11: Better monitoring system. Control room improvements. Improve SCADA system. Improve operator vigilance. Diagnostic capability via remote desktop or similar technology. HAZOP	Krennic	1.6.1

RECOMMENDATION	ASSIGNED TO	WORKSHEET PLACES USED
Update: No additional safeguards considered necessary, PHA action closed		1.7.1
12: Mechanical/system interlock. Automatic fail safes. HAZOP Update: No further safeguard considered necessary	Krennic	1.8.1
13: Control dial. Touchscreen interface. HAZOP Update: Carry out audit of maintenance records to identify root cause of ray shield jams. Ensure touchscreen software BIOS update has been implemented	Tarkin	1.4.1
14: Threshold warning system. Condition monitoring. System feedback. HAZOP Update: See new recommendation regarding overtemperature alarm / trip	Krennic	1.1.7
15: Safe zone – system optimization. Engineered level. HAZOP Update: Recommendation no longer applicable, considered closed	Krennic	
16: Liason between forcefield and exhaust port monitoring teams. Get the roids to do it…but don't trust them completely. HAZOP Update: See new recommendation re. Security Assessment	Krennic	1.8.2
17: Resolve discrepancy between design documentation (exhaust port 2m diameter) and 'as-built' (exhaust port shown up to 50m diameter)	Krennic	1.1.1
18: Carry out QA Audit of maintenance records to ensure that no detrimental repairs have been carried out	Krennic	1.1.3
19: Review if overtemperature alarm / trip is active, or if not available could be retrofitted (note: trip function should reduce core output, but not shut it down completely due to base load requirements of other Death Star consumers)	Krennic	1.5.1 1.1.3 1.1.6 1.1.7
20: If analysis shows that ingress of external material is physically possible (see recommendation below), then consider retrofitting particle shields on all exhaust ports	Tarkin	1.3.1
21: Align Imperial planet destruction strategy with operational limitations of Death Star	Darth Vader	1.5.1
22: Carry out security assessment as per IEC 61511-1, section 8.2.4	Krennic	1.1.7 1.8.2
23: Although the Ray Shield function is not strictly a SIF as per IEC 61511, it is recommended nevertheless to carry out LOPA to confirm that Safety Integrity Level is sufficient to bring residual risk to acceptable level (considering other IPLs)	Tarkin	1.4.1
24: Review if radiation pressure (photon momentum) counteracts ingress momentum of	Jason S	1.3.1

RECOMMENDATION	ASSIGNED TO	WORKSHEET PLACES USED
flotsam, i.e. pressure exceeds core gravity, resulting in an intrinsically safe system that prevents debris from reaching the core		
25: Review control hierarchy to ensure there is no common cause that leads to failure of complete heat rejection system (i.e. ensure local control is independent of central control)	Krennic	1.1.4
26: Ensure that mantenance plan limits the number of heat sinks that can be concurrently under maintenance	Krennic	1.1.5
27: Review increasing the number of fighters and / or turboblaster batteries to further reduce the frequency of successful attacks	Darth Vader	1.4.1

Appendix B Death Star - ReHAZOP Worksheets

Unit	DS-1 Orbital Battle Station
Process Type	
Process Mode	Unknown

Node	Thermal Exhaust Port - Expel excess energy (Task Step 2.1.1.5)	A thermal exhaust port is an outlet for dissipating the excess heat produced by the large energy reactors used on board starships and space stations or in certain ground-based structures. These ports draw excess heat energy away from the reactors and other equipment in a structure and expell it into space or the atmosphere to prevent damage to systems or injury to the crew from heat build-up. Small thermal exhaust ports (2m diameter) scattered over the Death Star's surface open upon shafts leading directly to the main reactor. Source: Wookieepedia
References		

Deviation	Cause	Consequence	Cat	L	S	Lw/SG	Rw/SG	Safeguard	Recom-mendation	LOPA	Comments
1. Less than	1. PHA: As-built Exhaust port too small (not matching to design plans). Amazing it works in the first place. Giant amount of energy.	1. Kill's everyone on board. Too hot/cold in a giant metal ball. Functions out of balance. General wear on essential part of station. Compounding problem of fixing problem might cause more exhaust emissions. HAZOP Update: Loss of single port results in only local harm to Personnel, therefore severity chosen as 5: Onsite fatalities	S	2	5	1	5	1. Sensing capabilities and control. HAZOP Update: temperature sensors available on each port, ALM 11. HAZOP Update: Numerous (redundant) exhaust ports are available, BU	1. 2. 3. 4. 17.	N/A	
	2. HAZOP Update: During normal operation - base load. Peak load when planets are destroyed. Not tested at full power during commissioning	1. Multiple fatalities throughout DS-1 due to interconnectivity of heat rejection system	S	3	6	2	16	13. Commissioning procedures, SAT, ADM	2.	N/A	
	3. HAZOP Update: Modification to system during operation (e.g. decoupling from heat sink), reducing capability of a single port, but	1. Could cause local overheating leading to damage, safety issue. Harm to personel in local City Sprawl area, potential injury	S	3	4	2	9	12. Management of Change, O&M records, ADM	18. 19.	N/A	

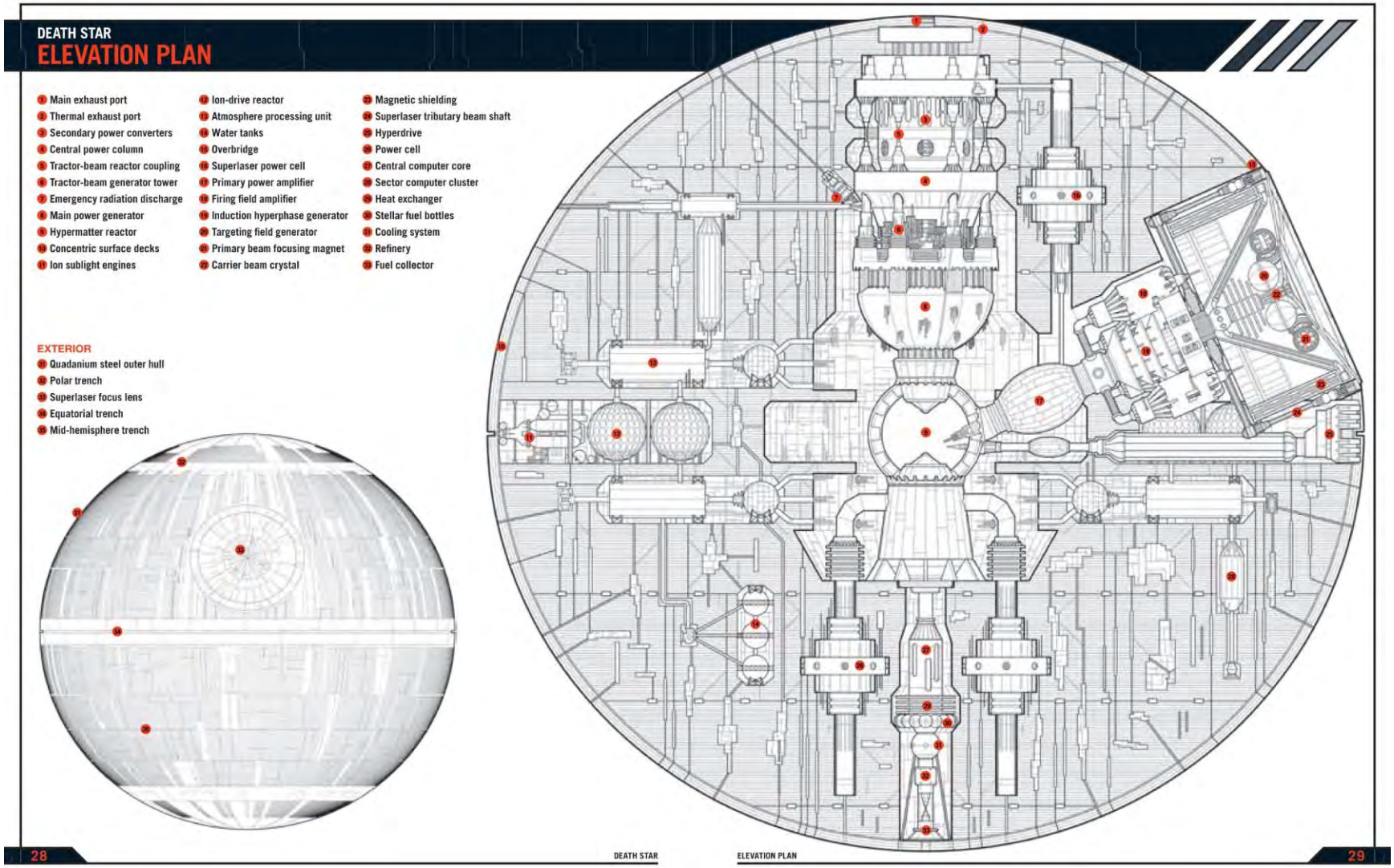
Deviation	Cause	Consequence	Cat	L	S	Lw/SG	Rw/SG	Safeguard	Recom-mendation	LOPA	Comments
	not limiting full capacity.										
	4. HAZOP Update: Surface heat sink capacity contoller fails (assumed local malfunction of a single port)	1. Could cause local overheating leading to damage, safety issue. Harm to personel in local City Sprawl area, potential injury	S	3	4	2	9	14. Standard Operating Procedures (SOP), ADM 12. Management of Change, O&M records, ADM	25.	N/A	
	5. HAZOP Update: Heat sink capacity significantly reduced due to longterm maintenance of numerous ports and immediate instruction to fire laser	1. Multiple fatalities throughout DS-1 due to interconnectivity of heat rejection system	S	3	6	2	16	12. Management of Change, O&M records, ADM	26.	N/A	
	6. PHA: Malfunction -> Fried equipment due to heat. HAZOP Update: Potential cause confirmed, however, Operational experience doesn't indicate any negative experience to date - Copy	1. Heat and radiation prevented from getting out – ray shield too strong. HAZOP Update: Could cause local overheating leading to damage, safety issue. Harm to personel in local City Sprawl area, potential injury	S	3	4	2	9	6. Reset strength of forcefield – quick disablement of port. Isolate problem. HAZOP Update: Operator intervention takes longer than 15 minutes, therefore this measure is not considered a safeguard as per IEC 61511, ALM 1. Sensing capabilities and control. HAZOP Update: temperature sensors available on each port, ALM	19.	N/A	
	7. PHA: Sabotage. Incompetence -> Controls set incorrectly. Malfunction. Push dial too far due to inattention or slip - Copy	1. Make problem worse. Make port vulnerable. Or make port less effective in dissipating heat. HAZOP Update: See consequences under GW 'More than'	S	4	4	3	14	6. Reset strength of forcefield – quick disablement of port. Isolate problem. HAZOP Update: Operator intervention takes longer than 15 minutes, therefore this measure is not considered a safeguard as per IEC 61511, ALM 1. Sensing capabilities and control. HAZOP Update: temperature sensors available on each port, ALM	14. 19. 22.	N/A	
2. More than	1. PHA: Power source. Optimum amount of energy balance is required, so becomes out of balance. HAZOP Update: Original PHA concern not clear. Guide Word 'More Than', it is understood that the concern	1. Too hot/cold in a giant metal ball. Functions out of balance. General wear on essential part of station. HAZOP Update: According to Operator feedback, overcooling the reactor has been experienced during operation and is not a safety concern	S	3	1	2	1	1. Sensing capabilities and control. HAZOP Update: temperature sensors available on each port, ALM		N/A	

Deviation	Cause	Consequence	Cat	L	S	Lw/SG	Rw/SG	Safeguard	Recom-mendation	LOPA	Comments
	is that more radiation is expelled than required, leading to overcooling of the reactor surface and deterioration of materials										
	2. HAZOP Update: Surface heat sink capacity contoller fails (assumed local malfunction of a single port)	1. Too hot/cold in a giant metal ball. Functions out of balance. General wear on essential part of station. HAZOP Update: According to Operator feedback, overcooling the reactor has been experienced during operation and is not a safety concern	S	3	1			12. Management of Change, O&M records, ADM 14. Standard Operating Procedures (SOP), ADM		N/A	
3. As well as	1. PHA: Floating space debris – but there is a force field. Poor design. Substandard materials. Cost cutting. Planning for maintenance in the future. Channel for something unwanted to enter like vermin or rubbish. Material properties of port constrains design. Bits of port fall off. Bits melt off and re-harden somewhere else. HAZOP Update: Potential cause confirmed, however, operating anecdotal experience to date indicates no issue with ingress of external material (however, there are no records to confirm if external material has in fact entered the port)	1. Kill's everyone on board. Too hot/cold in a giant metal ball. Functions out of balance. General wear on essential part of station. Compounding problem of fixing problem might cause more exhaust emissions. HAZOP Update: Loss of single port results in only local harm to Personnel, therefore severity chosen as 5: Onsite fatalities	S	4	5	3	16	2. Do a cognitive work analysis. HAZOP Update: not considered as a Safeguard to IEC 61511, 11. HAZOP Update: Numerous (redundant) exhaust ports are available, BU	5. 6. 7. 8. 20. 24.	N/A	Note: Ray shield is deflector type used to absorb radiation and raw energy by deflecting or scattering energy beams. Physical objects may pass through. Therefore not included as a safeguard for this cause. See GW 'Other Than'
4. Other than	1. PHA: Rebel Fleet close to the Death Star. HAZOP Update: Existing defences have repelled 22 Rebel Alliance attacks in 5 years. Operational experience does indicate some instances of ray shield jamming. There was	1. Degradation of port function due to attack, potential local harm to personnel. HAZOP Update: Noted that ray shield function is to deflect energy, not particles. See Node 1 Guideword 'As well as'. Consequence of port ray malfunction is that external laser attack may damage a sinlge exhaust port. See Node 1 Less	S	4	5	2	10	6. Reset strength of forcefield – quick disablement of port. Isolate problem. HAZOP Update: Operator intervention takes longer than 15 minutes, therefore this measure is not considered a safeguard as per IEC 61511, ALM 7. Complement of TIE fighters that	13. 23. 27.	Yes	Ref: 'How a Bowtie Diagram could have saved the Death Star', David Jamieson. There was a long discussion amongst the Team regarding double jeopardy. HAZOP Chairman referred to

Deviation	Cause	Consequence	Cat	L	S	Lw/SG	Rw/SG	Safeguard	Recom-mendation	LOPA	Comments
	insufficient information about the attack frequency to allow HAZOP Team to ascertain the number of attacks specifically on the exhaust ports. Therefore the frequency of an attack that could potentially cause damage to a port was estimated as 1 every 100 years	Than						can be deployed to engage the rebel fleet., ADM 8. Superlaser with enough power to destroy an entire planet. HAZOP Update: Superlaser ineffective against Rebel Starfighter. Not considered as a safeguard, 9. 15000 turboblaster batteries, OTH 10. Thermal exhaust port is only 2m wide. Rebel fighter could not get close enough. HAZOP Update: Not considered as a safeguard, 15. Ray shield protection for exhaust ports, IPF			introductory remarks: 'Double jeopardy' failure and failure of safety system can be potential causes. In this case Initiating Event (Rebel Attack) and failure of protection system (Ray Shield) are NOT independent events.
	2. HAZOP Update: Team reviewed potential common cause failure that would result in significantly reduced cooling capacity and could not find a plausible cause	1. Core out of control, complete destruction of the Death Star	S		6					N/A	
5. Repeated	1. PHA: Over- zealous with the super laser. Over use of the weapon creates too much thermal energy/radiation – needs a cool down period. -> Access gate to exhaust port activating too much. HAZOP Update: Potential cause (overheating) confirmed, local Operators confirm contradictory command requests, potentially indicating managerial misunderstanding of superlaser technical limitations. Note: there is no access gate to the exhaust port that activates	1. Multiple fatalities throughout DS-1 due to interconnectivity of heat rejection system	S	3	6	2	16	3. Stop over using it. Full shut down. Re-boot Death Star. HAZOP update: not a valid safeguard because: 1. Management overrides operational limits. 2. Death Star cannot be completely shut down and rebooted, 1. Sensing capabilities and control. HAZOP Update: temperature sensors available on each port, ALM	9. 10. 21. 19.	N/A	
6. Sooner	1. PHA: Lack of sensing capability -> Poor control.	1. Wasting energy and output. HAZOP	S	4	1	4	1	4. Human (alien) intervention of some sort. HAZOP Update: Not	11.	N/	

Deviation	Cause	Consequence	Cat	L	S	Lw/SG	Rw/SG	Safeguard	Recom-mendation	LOPA	Comments
than	Hazop update: see new causes below	Update: see below						considered as a safeguard, ,		A	
	2. HAZOP Update: Heat sink capacity increased before it is required ->overcooling	1. See More Than	S							N/A	
	3. HAZOP Update: Heat sink capacity reduced before it is required ->overheating	1. See Less Than	S							N/A	
7. Later than	1. PHA: Lack of sensing capability -> Poor control	1. Don't want too much energy in the core. Might slow things down, effect system performance. Strains systems if too much. HAZOP Update: potential overheating -> affecting capacity of singl eport (see Less Than)	S	3	4	2	9	4. Human (alien) intervention of some sort. HAZOP Update: Not considered as a safeguard, 14. Standard Operating Procedures (SOP), ADM 1. Sensing capabilities and control. HAZOP Update: temperature sensors available on each port, ALM	11.	N/A	
8. Misordered	1. PHA: Faulty mechanics. Something not opening. Faulty sensors -> Energy for laser being expelled out of exhaust port and wasted. HAZOP update: cause no longer considered valid - see Sooner than / Later than	1. Don't want energy for laser to shoot out of exhaust port and be wasted. Diminishes ability of the Death Star to fire main weapon system. HAZOP Update: Not a safety concern	S					5. Shut it all down and re boot, ALM 14. Standard Operating Procedures (SOP), ADM	12.	N/A	
	2. PHA: Other warnings and control room ergonomics. Other demands and priorities. Workload and teamworking. Under staffing -> Distraction, concurrent demands, operator forgets what they are doing, error of commission. HAZOP Update: Operational error confirmed as valid cause	1. Kill's everyone on board. Too hot/cold in a giant metal ball. Functions out of balance. General wear on essential part of station. Compounding problem of fixing problem might cause more exhaust emissions. Destroys main power generator. Puts life support at risk.	S	3	6	2	16	6. Reset strength of forcefield – quick disablement of port. Isolate problem. HAZOP Update: Operator intervention takes longer than 15 minutes, therefore this measure is not considered a safeguard as per IEC 61511, ALM 1. Sensing capabilities and control. HAZOP Update: temperature sensors available on each port, ALM	16. 22.	N/A	

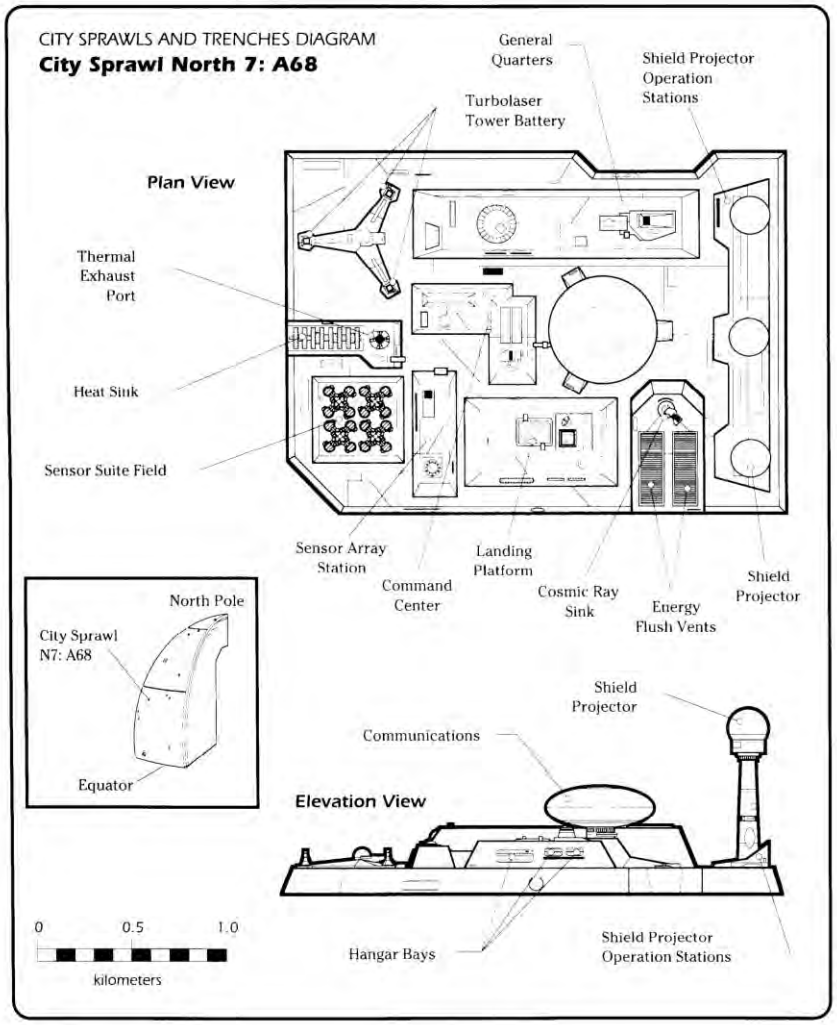
Appendix C Death Star - ReHAZOP Documentation



Source: Imperial Death Star - Owner's Workshop Manual © Haynes

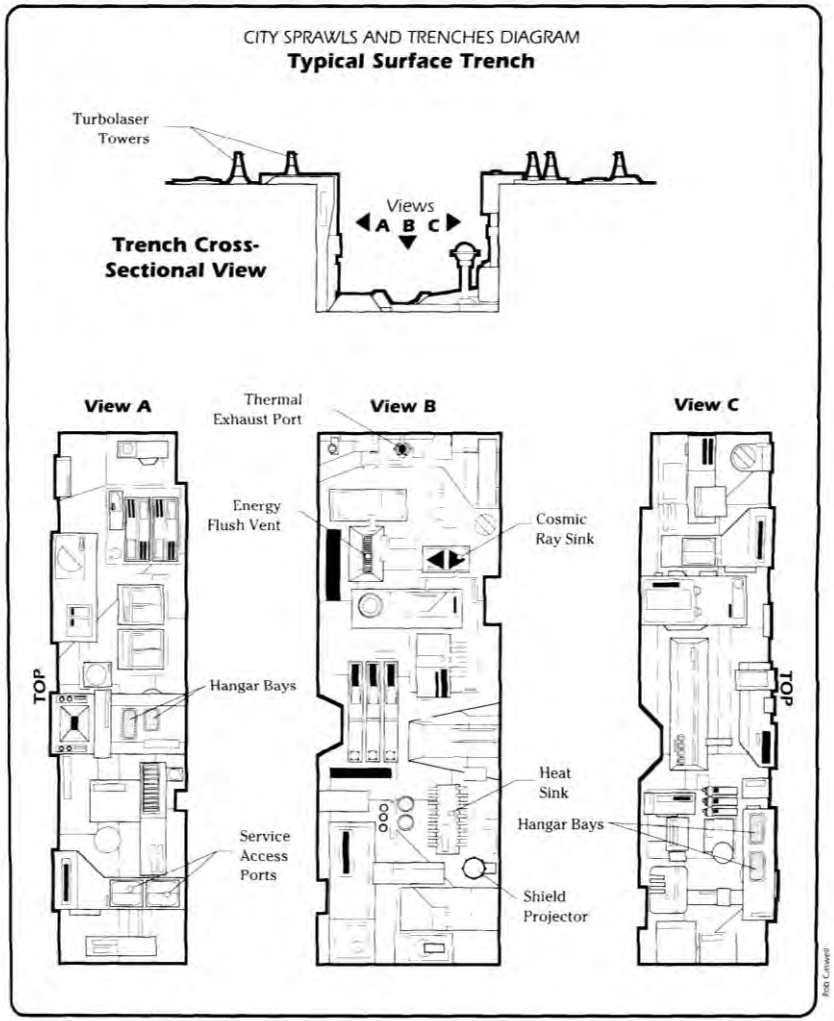
CITY SPRAWLS AND TRENCHES DIAGRAM

City Sprawl North 7: A68



CITY SPRAWLS AND TRENCHES DIAGRAM

Typical Surface Trench



Source: Death Star Technical Companion © West End Games