Introduction to systems safety engineering

Introduction to Systems Safety Engineering ISE 741 North Carolina State University ISE 741, Fall 2012 • Faculty Introduction – Dr. Nancy Currie – Dr. David Kaber – Dr. Guk-Ho Gil http://www. jsc. nasa. gov/Bios/htmlbios/currie. html http://people. engr. ncsu. edu/dbkaber/ http://www. ise. ncsu. edu/people/staff/gil. php http://courses. ncsu. edu/ise741/lec/001/ • Course Website – Course Syllabus – Communication Information http://courses. ncsu. edu/ise741/lec/001/Internet_info_fall2012_ISE741. pdf http://courses. ncsu. edu/ise741/lec/001/ISE%20741%20syllabus. pdf – Course Schedule http://courses. ncsu. du/ise741/lec/001/ISE%20741%20Course%20Schedule. pdf • Course Topics Course Topics • Systems Safety Process • Hazard Reduction & Safety Standards • Safety Management • Preliminary Hazard List (PHL) • Preliminary Hazard Analysis (PHA) • Subsystem Hazard Analysis (SSHA) • System Hazard Analysis (SHA) • Process Safety Analysis • Probability & Reliability review • Failure Modes & Effects Analysis (FMEA) • • • • • • • • Boolean Logic Review Fault Tree Analysis (FTA) Cut Sets & Path Sets Software Safety Analysis Energy Trace Barrier Analysis Sneak Circuit Analysis Probabilistic Risk Assessment (PRA) Accident Investigation and Reporting

Perspectives on Systems Safety Engineering • “ As our technology expands, as our wars multiply, and as we invade more and more of nature, we create systems – organizations, and the organization of organizations – that increase our risk for the operators, passengers, innocent bystanders, and for future generations. ” – Charles Perrow, Normal Accidents “ Although many designers can appreciate the difficulty of creating designs without hazards or with effective guards, few designers have a basis (or the expertise) to

understand the complexities of designing a warning. – Ward Allen, “ What do design engineers really know about safety? ” • • “ If a sufficient number of management layers are superimposed on top of each other, it can be assured that disaster is not left to chance. ” – Norm Augustine, Augustine Laws “ Complex systems almost always fail in complex ways. ” – Columbia Accident Investigation Board and National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling • Definitions “ System” A composite, at any level of complexity, of personnel, procedures, materials, tools, equipment, facilities, and software.

The elements of this composite entity are used together in the intended operational or support environment to perform a given task or achieve a specific production, support, or mission requirement. “ System Safety” The application of engineering and management principles, criteria and techniques to achieve acceptable mishap risk, within the constraints of operational effectiveness and suitability, time and cost, throughout all phases of the system life cycle Definitions “ Systems Safety Engineering”

The application of scientific and engineering principles, criteria, and techniques to identify and eliminate hazards, in order to reduce the associated risk through: ? Identification of systems hazards and associated causes ? Development of engineering, operational, or management controls to either eliminate hazards or mitigate their consequences ? Evaluation of the strength of control measures ? Continual monitoring of the system to determine any changes in hazards or associated controls “ Risk Assessment”

The process of characterizing hazards within risk areas and critical technical processes, analyzing them for their potential mishap severity and probabilities of occurrence, and prioritizing them for risk mitigation actions * Hazard is a generic reference to potential causal factors of accident scenarios, whether direct or indirect, primary or contributory. Historical Perspective of Systems Safety Engineering • Code of Hammurabi – ~1750 BC • First laws covering compensation for injuries codified – Middle Ages • Lloyd’s Register of British and Foreign Shipping created – ~1834 – institutionalized concept of safety and risk analysis US National Safety Council founded – 1913 • US Air Force published “ System Safety Engineering for the Development of Air Force Ballistic Missiles” – 1962 – Minuteman Intercontinental Ballistic Missile (ICBM) first to have a formal systems safety program • Mil-Std-882, “ Requirements for System Safety Program for Systems and Associated Subsystems and Equipment”, first published – 1969 – Considered a primary reference for system safety – Latest revision (MIL-STD-882E) – released May 2012 System Safety Program Objectives Safety, consistent with mission requirements, is designed into the system in a timely, cost-effective manner • Hazards associated with each system, subsystem and component are identified, tracked, evaluated, and eliminated or controlled to an acceptable level throughout the lifecycle of the system • The safety design order of precedence is applied and controls for hazards that cannot be eliminated are established to protect personnel, equipment, property, and/or environment • Changes in design, configuration, or operations required to improved safety are minimized through the timely inclusion of safety factors during the acquisition of a system • Minimum risk is involved in the acceptance and use of new materials and new production

and testing techniques • Historical safety data, including lessons learned from similar systems, are considered and used in safety assessments and analyses, where appropriate Why Systems Safety Engineering? System Safety Practice is required by… Prudent engineering practice – especially in high risk systems • Dictated by regulatory standards – – 21 CFR 807. 87 (g) – requires hazard analyses as a part of " premarket notification" for medical devices – 29 CFR 1910. 119 (e) (2) – requires applying " one or more… methodologies to determine and evaluate…hazards…" – 29 CFR 1910. 146 (b) (4) – requires identifying hazards in " permitrequired confined spaces [containing] any…recognized serious safety or health hazard. " – DODI 5000. 36 – requires system safety programs for many system acquisitions (Ref. MIL-STD-882D) – NASA NPG 8715. 3; Chapter 3 – " System Safety" Simple Event Chain BREACHED CONTROL Hazard Event Target BREACHED DEFENSE

Incident Trajectory – how event chains can lead to incidents/accidents TARGET (personnel) HAZARD (Ignition source) TARGET (flammable material) HAZARD (ineffective medical response) EVENT-TARGET (Personnel burned) Intermediate Events EVENT (Partial disability) EVENTHAZARD (fire) Preliminary/ Initiating Event TARGET (equipment) Final Event EVENT (Equip damaged) Example – Elements of an Explosion Event • Hazards – Flammable/combustible/unstable materials – Inert gases • Initiating events – Malfunctioning pumps, valves, instruments, sensors • Propagating events – Deviations of pressure, temperature, flow, rate, concentration, phase/state change • Ameliorative events – Redundant components, relief valves, redundant systems, redundant utilities Deepwater Horizon Accident – 2010 On the evening of April 20, 2010, a well control event allowed hydrocarbons

to escape from the Macondo well onto Transocean’s Deepwater Horizon, resulting in explosions and fire on the rig – – The fire, fed by hydrocarbons from the well, continued for 36 hours until the rig sank 11 people were killed and 17 were injured • The accident chain of events: ? Well integrity failure ? Loss of hydrostatic control of the well ? Failure to control the flow from the well with the blowout preventer equipment, which allowed the release and subsequent ignition of hydrocarbons ? BOP emergency functions failed to seal the well after the initial explosions • •

Hydrocarbons continued to flow from the reservoir through the wellbore and the blowout preventer for 87 days, causing an oil spill of national significance The accident investigation team used fault tree analysis to define and consider various failure scenarios, failure modes, and possible contributing factors Deepwater Horizon Accident – 2010 ? Well integrity failure • Results of the negative pressure test were incorrectly accepted by BP and Transocean ? Well integrity had not been established ? Loss of hydrostatic control of the well • Cement and shoe track barriers, in particular the cement slurry that was used at the bottom of the well, failed to contain hydrocarbons within the reservoir ?

Gas and liquids allowed to flow up the production casing • Over a 40-minute period, the Transocean rig crew failed to recognize and act on the influx of hydrocarbons into the well ? Hydrocarbons were in the riser and rapidly flowing to the surface ? Failure to control the flow from the well with the blowout preventer (BOP) equipment, which allowed the release and subsequent ignition of hydrocarbons • After the well-flow reached the rig it was routed to a mud-gas separator, causing gas to be vented directly on to

the rig rather than being diverted overboard ? Flow of gas into the engine rooms through the ventilation system created a potential for ignition which the rig’s fire and gas system did not prevent ?

BOP emergency functions failed to seal the well after the initial explosions • Critical components of the BOP were inoperable ? After explosion and fire had disabled crew-operated controls, the rig’s BOP on the sea-bed did not activate automatically, as designed, to seal the well Risk Decisions Related to Deepwater Horizon Accident DECISION LESS RISKY ALTERNATIVE AVAILABLE? Yes Yes LESS TIME THAN ALTERNATIVE Saved Time Saved Time DECISION-MAKER Not waiting for more centralizers of preferred design Not waiting for foam stability test results and/or redesigning slurry Not running cement evaluation log BP on Shore Halliburton (and Perhaps BP) on Shore BP on Shore • No formal system for ensuring that alternative procedures were in fact equally safe Yes Saved Time

Using Spacer Made from Combined Lost Circulation Materials to Avoid Disposal Issues Displacing Mud from Riser Before Setting Surface Cement Plug Setting Surface Cement Plug 3, 000’ Below Mud Line in Seawater Not Installing Additional Physical Barriers During Temporary Abandonment Procedure Not Performing Further Well Integrity Diagnostics in Light of Troubling and Unexplained Negative Pressure Test Results Bypassing Pits and Conducting Other Simultaneous Operations During Displacement Yes Yes Yes Yes Yes Saved Time Unclear Unclear Saved Time Saved Time BP on Shore BP on Shore BP on Shore BP on Shore BP (and perhaps Transocean) on rig Transocean (and perhaps BP) on rig No comprehensive and systematic risk-analysis, peerreview, or management of change process • No formal

analysis to assess the relative riskiness of available alternatives Yes Saved Time “ Whether purposeful or not, many of the decisions that BP, Halliburton, and Transocean made that increased the risk of the Macondo blowout clearly saved those companies significant time and money. ” – National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling System Safety Process Define Objectives System Description System/Process Review Hazard Identification Hazard Analysis Risk Assessment Hazard Controls Evaluation/Validation of Define Objectives Hazard Control Is risk acceptable? No Risk Management Documentation Risk Management Modify System/ Process Yes Risk Acceptance & Rationale Documentation