MAINTAINING SAFETY IN FUTURE GAS SYSTEMS

The Need to Include Systemic Risk Assessments

Ben Riemersma
Delft University of Technology
2020 MIT Workshop (July 27th)

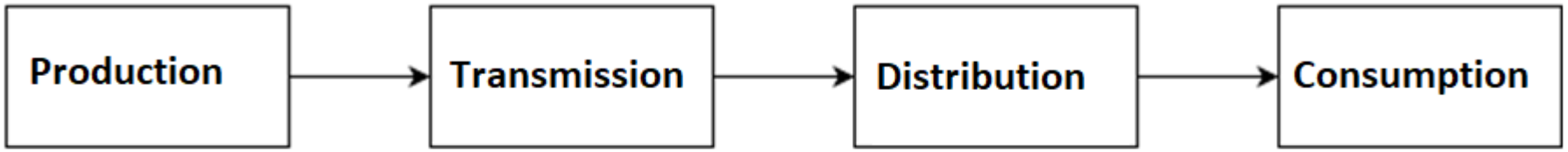
How can we assess risks in complex gas systems?

Outline

- Gas Systems
- Risk Assessments
- Conclusion

Gas Systems (1/2)

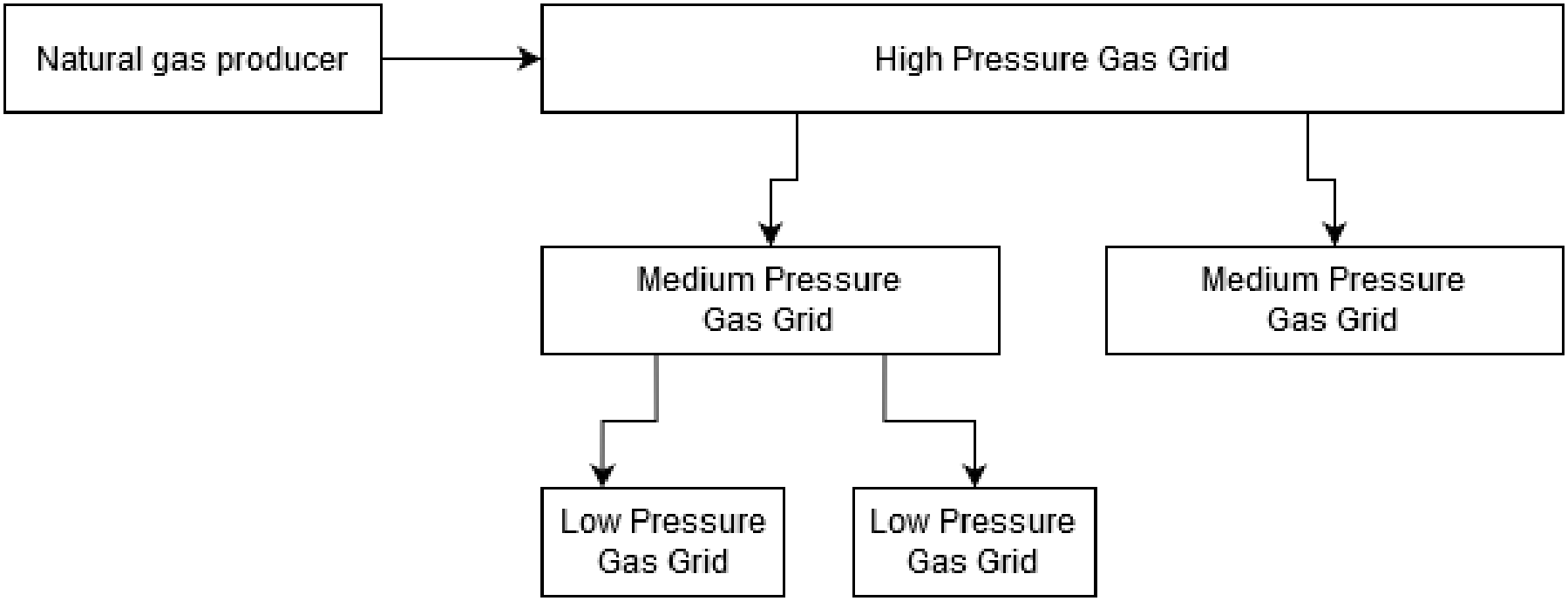
Conventional Gas System



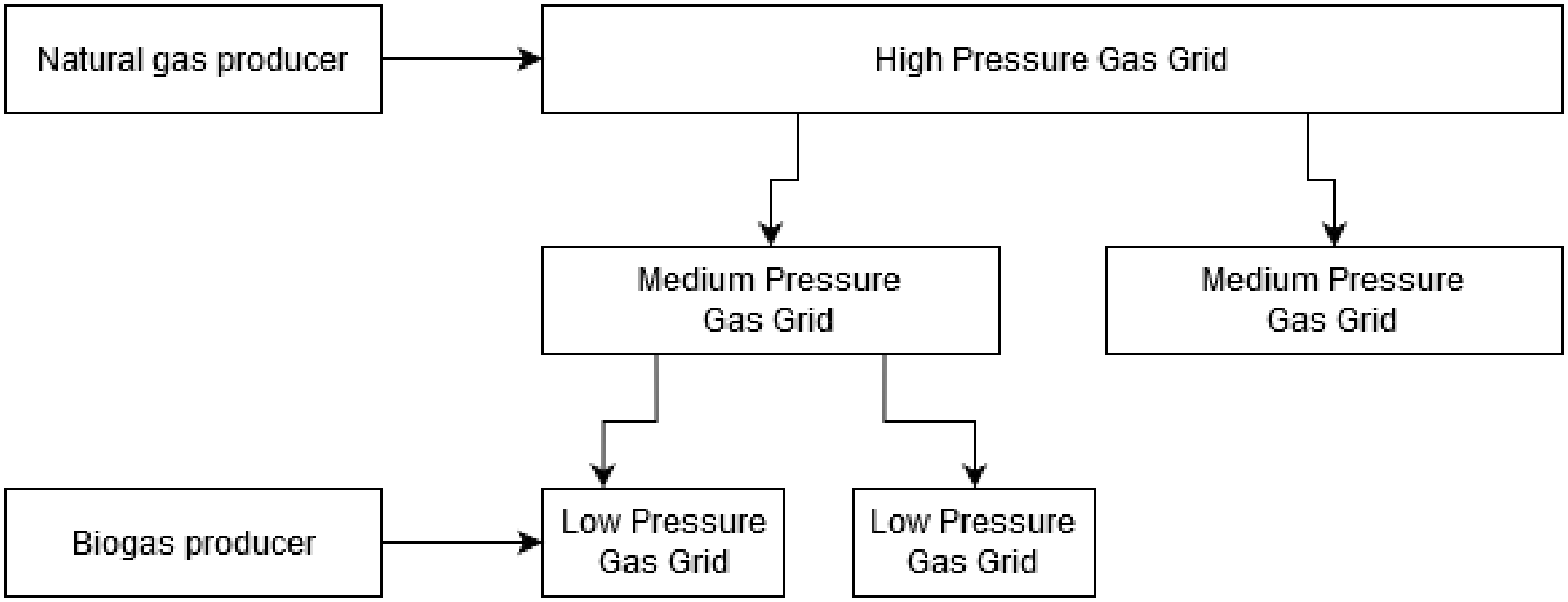
Gas Systems (2/2)

- Increasingly characterized by
  - Non-linear interactions
  - Feedback loops
  - Interconnected subsystems

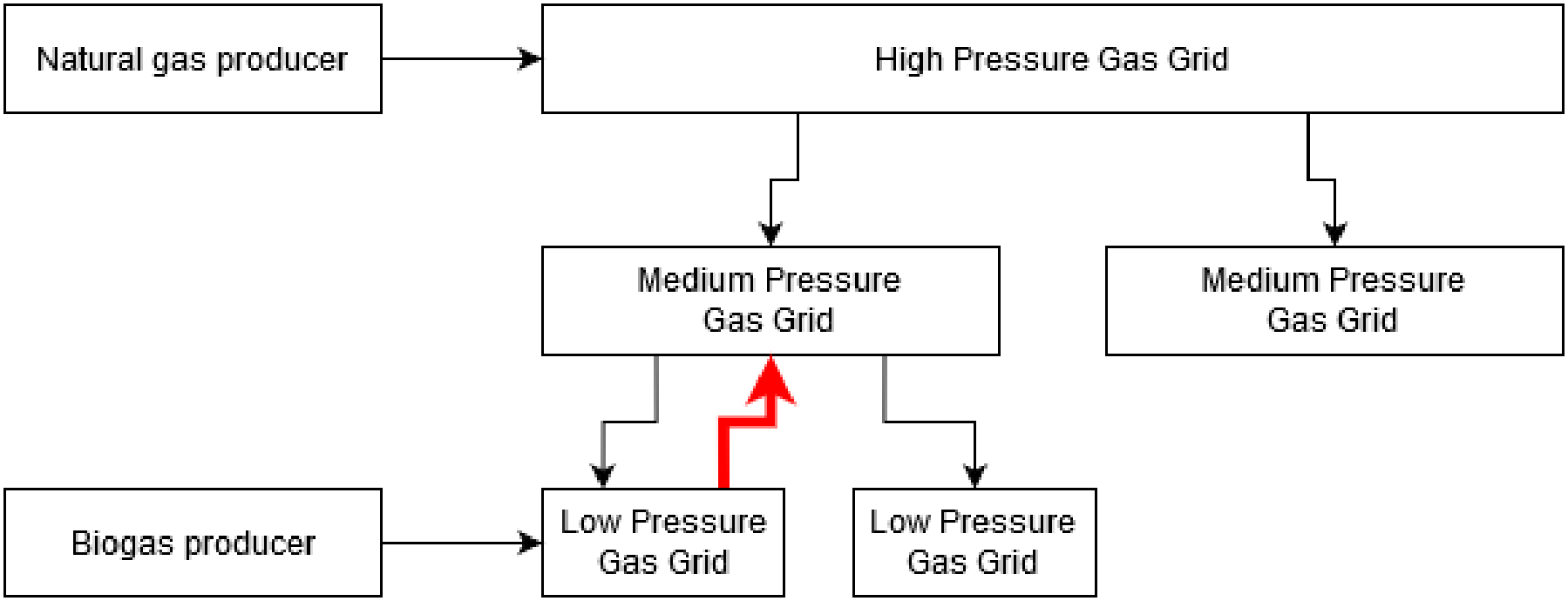
Gas Booster


Natural gas producer
High Pressure Gas Grid
Medium Pressure Gas Grid
Medium Pressure Gas Grid
Low Pressure Gas Grid
Low Pressure Gas Grid

Gas Booster


Natural gas producer
High Pressure Gas Grid
Medium Pressure Gas Grid
Medium Pressure Gas Grid
Biogas producer
Low Pressure Gas Grid
Low Pressure Gas Grid

Gas Booster


Natural gas producer
High Pressure Gas Grid
Medium Pressure Gas Grid
Medium Pressure Gas Grid
Biogas producer
Low Pressure Gas Grid
Low Pressure Gas Grid

Risk Assessments

- Hazard and Operability Study (HAZOP)
  - Executed by grid operator
  - Focus on gas booster

- System-Theoretic Process Analysis (STPA)
  - Executed with grid operator
  - Focus on effects of gas booster

Pressure: Hazards and Accidents

HAZOP	STPA
Incoming pressure too high	*Gas pressure in source grid leaves acceptable boundary levels*
• Unfiltered gas in system • Gas escapes system	• Fire/Explosion • Poisoning • Loss of operator revenue • Loss of producer revenue

Pressure: Hazards and Causes

HAZOP	STPA
Incoming pressure too high	*Gas pressure in source grid leaves acceptable boundary levels*

Pressure: Hazards and Causes

HAZOP

Incoming pressure too high

- 4 bar grid pressure too high
- Pressure regulator defective
- Pressure regulator out-of-spec

STPA

Gas pressure in source grid leaves acceptable boundary levels

UCA-1-SCENARIOS

- *Software is installed so that abort/decrease cmd. overrides initiate cmd. (possible conflicting parameters: destination grid pressure > 8.2 bar; gas is off-spec)*
- *Process model regarding source grid pressure is wrong*
- *Process model regarding destination grid pressure is wrong*
- *Process model regarding gas quality is wrong*
- *Control algorithm sends inappropriate CA based on inconsistent process model or faulty design*
- *Hostile takeover (computer hack) leads to inappropriate CA*
- *Initiate cmd. not (or too late) received by remote control*
- *Remote control delays sending initiate cmd.*
- *Compressor fails to follow up on initiate cmd.*
- *Off-spec gas is detected at compressor (i.e. continuous gas quality sensor is defective; power outage but gas keeps flowing; shut-off valve is defective)*
- *Gas that is sent to the grid becomes off-spec before it reaches the compressor*
- *Compressor failure*
- *Power outage (but biogas production continues)*
- *Changing supply and demand increase gas pressure in segments of the grid not registered by the sensor*
- *Sensor fails to measure grid capacity correctly*
- *Sensor fails due to power outage*
- *Sensor sends faulty or no information regarding grid pressure*
- *Mechanical stop is shut in the compressor*
- *Multiple boosters (or large biogas producers) are connected to one destination grid and have priority*

Pressure: Hazards and Causes

HAZOP	STPA
Incoming pressure too high	*Gas pressure in source grid leaves acceptable boundary levels*
• 4 bar grid pressure too high • Pressure regulator defective • Pressure regulator out-of-spec	• Hostile takeover (computer hack) leads to inappropriate CA

Quality: Hazards and Accidents

HAZOP	STPA
Outgoing gas too warm	*Feeding in of out-of-spec gas into the destination grid*
• Gas escapes system • Gas degrades infrastructure and attached appliances	• Fire/Explosion • Poisoning • Loss of operator revenue

Quality: Hazards and Causes

HAZOP	STPA
Outgoing gas too warm	*Feeding in of out-of-spec gas into the destination grid*

Quality: Hazards and Causes

HAZOP

Outgoing gas too warm

- Cooling not functioning
- Heat exchange not functioning

STPA

Feeding in of out-of-spec gas into the destination grid

UCA-33 SCENARIOS

- Software is installed so that initiate cmd. overrides abort/decrease cmd. (possible conflicting parameters: source grid pressure >3.8 bar;
- Process model regarding gas quality is wrong (critical parameters are not tested)
- Control algorithm sends inappropriate CA based on inconsistent process model or faulty design
- Hostile takeover (computer hack) leads to inappropriate CA
- Abort or Decrease cmd. not (or too late) received by remote control
- Remote control delays sending Abort or Decrease cmd.
- Compressor fails to follow up on Abort or Decrease cmd.
- Off-spec gas is sent to the grid (i.e. continuous gas quality sensor is defective; power outage but gas keeps flowing; half-yearly parameters not frequent enough due to changing gas biomass source; shut-off valve is defective)
- Gas that is sent to the grid becomes off-spec before it reaches the compressor
- Compressor failure
- Sensor for quality control fails due to power outage (but biogas production continues)

Quality: Hazards and Causes

HAZOP	STPA
Outgoing gas too warm	*Feeding in of out-of-spec gas into the destination grid*
• Cooling not functioning • Heat exchange not functioning	• Process model regarding gas quality is wrong (critical parameters are not tested)

Conclusion

- Systemic hazards not adequately covered by HAZOP
  - Separately identified by HAZOP team
- STPA complementary
  - “Not-yet-hazards”
  - Use of software

Questions?

b.riemersma@tudelft.nl