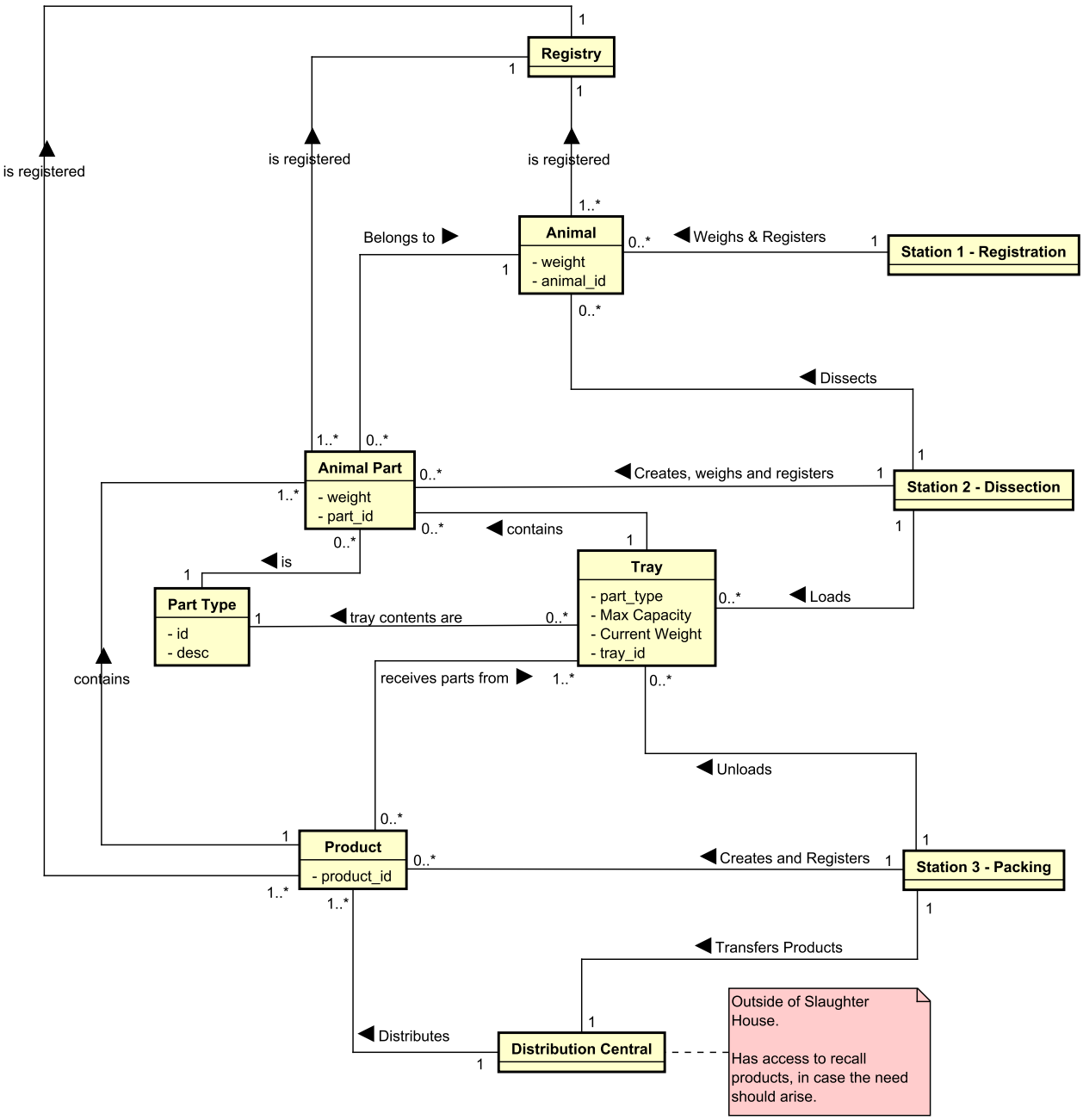
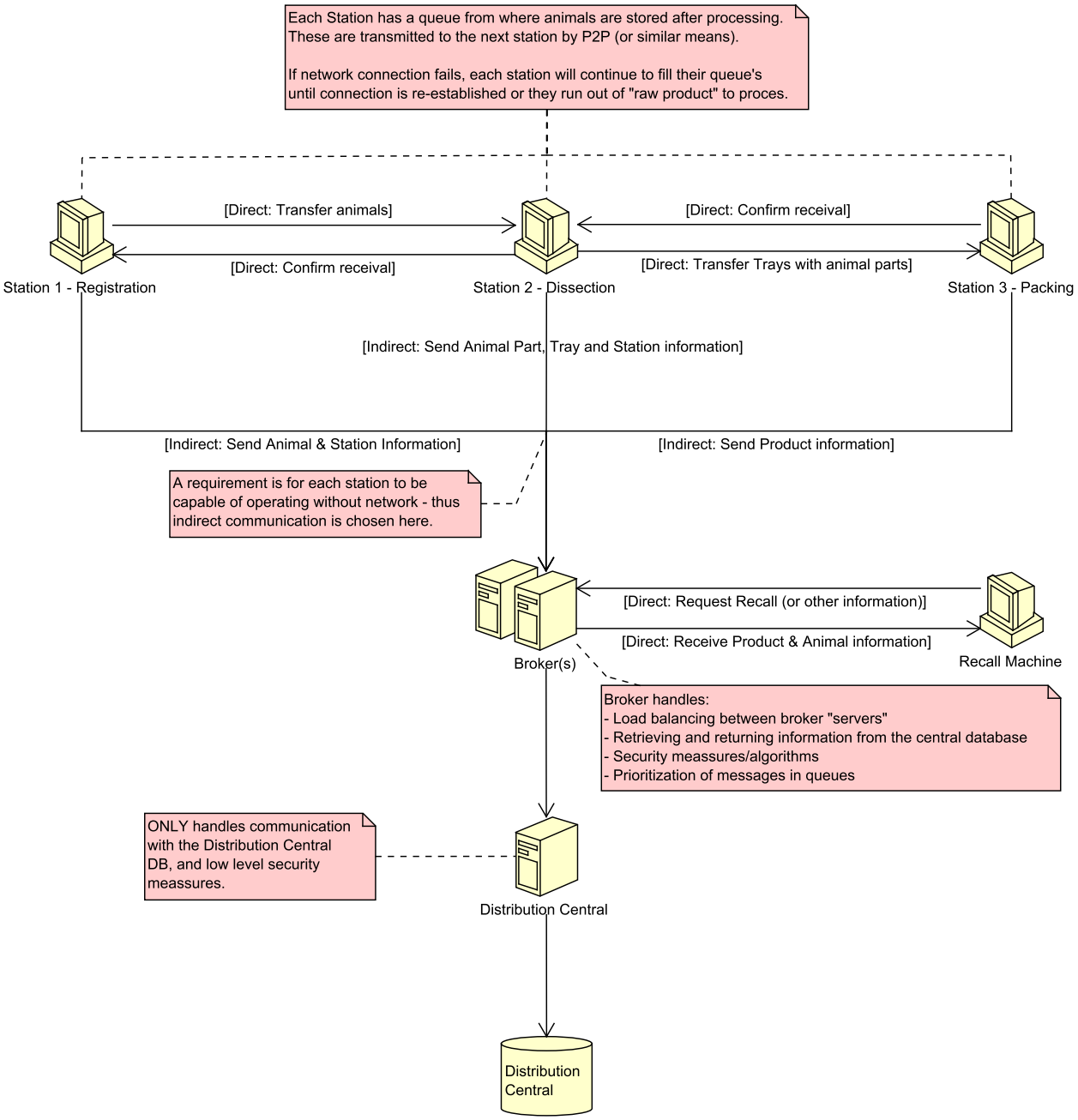
UML Domain Model:



Architecture Diagram:



Threat Model:

EINOO: Potential Attacker Analysis	
External Threats	1. Hackers, with an economical interest – or a political agenda (PETA or similar). 2. Foreign State Sponsored Agents, with the purpose of harming regional food supply. 3. Competitors, with the purpose of gaining insight in business secrets, statistics, production methods, etc.
Internal Threats	1. Current or just fired employees who might harbor bad intentions towards the company. 2. Employees who do not follow good practices relating to; a. passwords, b. data security, c. storage of company IT systems (computers), d. etc.
Network Threats	1. Connection to local power supply fails. 2. Network connectivity failure; stations cannot communicate with servers/brokers or other stations. 3. Database failure (For whatever reason, datacenter failure, power failure at datacenter, etc.)
Offline Threats	1. Physical theft of database 2. Physical sabotage of stations or broker/server infrastructure 3. Force majour (Fire, Natural Catastrophees, etc.) 4. Physical manipulation of IT infrastructure (USB's, theft of harddrives, etc.)
Online Threats	1. Hacking, 2. Online attacks/penerations on running systems, 3. Datamanipulation

STRIDE: Security Design Considerations	
Spoofing Identity	1. Protect against un-authorized actors who ”pretend” to be valid running stations or systems in order to add malicious data to the database. 2. Protect againsts un-authorized actors ”pretend” to be an authorized system with access to ’product recall’ functionality and data extraction from database or servers.
Tampering	1. Protect against manipulation of data through the brokers and other systems.
Information Disclosure	1. Protect against unintentional loss of business information, which might cause business secrets to be exposed, production/earnings statistics to be leaked, or similar consequences that might affect company value and reputation.
Denial of Service	1. Protect against DoS attacks on the brokers, who communicate with the database connected server, from external actors.
Elevation of Privilege	1. Protect against stations or clients gaining access to features and data restricted to certain users or stations; example: station 1 suddenly registering data that belongs to station 3, or unauthorized clients gaining access to ’recall product’ functionality. 2. Protect against assuming unauthorized roles that give access to data manipulation in the database.