- **DevOps blends the processes of development, quality assurance, and production**
  - **Steady collaboration between systems engineers, developers, testers, system administrators, and product owners, organized and focused by scrum masters, with an eye to deploying small components of functionality rapidly to the user community**
  - **Embed system administrators and other stakeholders into the development process**
  - **Developers need to understand what is happening in the production environment**
- **Blending of development and operation provides a framework for rapid feedback on the quality of software in the field**
- **Requires harmonic collaboration and frequent supervision in order to work out well.**

DevOps Principles

UNIVERSITY OF PASSAU
Faculty of Computer Science and Mathematics

- **Automate**
- **Blend operations, Quality Assurance, and development**
- **Instrument and provide continuous feedback**
- **Be transparent**
- **Be vigilant**

Required Properties

UNIVERSITY OF PASSAU
Faculty of Computer Science and Mathematics

- Security
  - Threat modelling
  - Attack tree
  - Automated security analysis
- Safety
  - Hazard analysis
  - Fault tree
- Resilience
  - Anticipate
  - Withstand
  - Recover
  - Evolve

Formulating Basic / Best Security Practices

UNIVERSITY OF PASSAU
Faculty of Computer Science and Mathematics

- Experience (lessons learnt)
- Expertise (systemic approach)
- Common security practices (systemic approach)
- IoT-specific approaches

Basic / Best Security Practices

UNIVERSITY OF PASSAU
Faculty of Computer Science and Mathematics

- Security should be enforced in IoT throughout the development and operational lifecycle of all IoT devices and hubs.
- The software running on all IoT devices should be authorized and authenticated.
- When an IoT device is turned on, it should first authenticate itself into the network before collecting or sending data.
- IoT devices have limited computation and memory capabilities, firewalling is necessary in IoT networks to filter packets directed to the devices.
- Updates and patches on the device should be installed in a way that additional bandwidth is not consumed and they should be authenticated.

Concerns

UNIVERSITY OF PASSAU
Faculty of Computer Science and Mathematics

- Speed to market matters
- Internet-connected devices face a deluge of attacks
- The IoT introduces new threats to user privacy
- IoT products and systems can be physically compromised
- Consumer convenience (UX – User eXperience)
- Skilled security engineers are hard to find (and retain)

Consumer Convenience

UNIVERSITY OF PASSAU
Faculty of Computer Science and Mathematics

- Easy installation and operation
- Plug ’n’ Play
- No complaints, no returns
- Poor customer knowledge
- Poor installation
- Poor technology understanding
- Applying best practices

Secure Design Goals

UNIVERSITY OF PASSAU
Faculty of Computer Science and Mathematics

- Design IoT systems that mitigate automated attack risks
- Design IoT systems with secure points of integration
- Design IoT systems to protect confidentiality and integrity
  - Applying cryptography to secure data at rest and in motion
  - Enabling visibility into the data life cycle and protecting data from manipulation
  - Implementing secure over-the-air updates
- Design IoT systems that are safe

Secure Design Goals

UNIVERSITY OF PASSAU
Faculty of Computer Science and Mathematics

- Design IoT systems using hardware protection measures
  - Introduce secure hardware components within your IoT system
  - Incorporate anti-tamper mechanisms that report and/or react to attempted physical compromise

- Design IoT systems that remain available
  - Cloud availability
  - Guarding against unplanned equipment failure
  - Load balancing

- Design IoT systems that are resilient
  - Protecting against jamming attacks
  - Device redundancy
  - Gateway caching
  - Digital configurations
  - Gateway clustering
  - Rate limiting
  - Congestion control
  - Provide flexible policy and security management features to administrators
  - Provide logging mechanisms and feed integrity-protected logs to the cloud for safe storage

Secure Design Goals

UNIVERSITY OF PASSAU
Faculty of Computer Science and Mathematics

- Design IoT systems that are compliant
  - The US IoT Cybersecurity Improvement Act of 2020
  - The baseline security recommendations of the European Union Agency for Cybersecurity (ENISA)
  - The US Department of Homeland Security (DHS) guiding principles for secure IoT
  - The US Food and Drug Administration (FDA) guidance on IoT medical devices