Health and Technology manuscript No.
(will be inserted by the editor)

Risk Analysis for the Design of a Safe Artificial Pancreas Control System

First Author · Second Author

Received: date / Accepted: date

Abstract Closed-loop glucose control has the potential to improve the glycemic control in patients with diabetes mellitus type 1. Such an artificial pancreas (AP) should keep the user safe despite all disturbances and faults. The objective of this paper is to analyze those perturbations according to their effects on the glycemic status, and thereby supporting an informed design process of the control system. As suggested by the international standard ISO 14971 for risk management of medical devices, the well proven failure modes and effects analysis (FMEA) was chosen as instrument. An FMEA scheme was modified for this purpose and applied to a single-hormone system with subcutaneous and intraperitoneal routes for glucose sensing and insulin administration. Faults that imply urgent danger and thus require fast detection and diagnosis were identified and distinguished from disturbances that can be sufficiently addressed by basic control functions, e.g. by adaptive control algorithms. Requirements and testing criteria for basic control functions as well as fault detection and diagnosis functions can be derived from the provided overview.

Keywords First keyword · Second keyword · More

1 Introduction

Safety is the primary requirement on a control system that doses insulin to regulate the blood glucose level (BGL) in diabetes mellitus type 1 (DM1). People with DM1 have an insufficient pancreatic insulin production and depend on lifelong insulin administration to avoid hyperglycemia. The chronically elevated BGL would otherwise lead to several long-term complications. Hypoglycemia caused by overdosing of insulin, on the other hand, may lead to unconsciousness and death in the

F. Author
first address
E-mail: fauthor@example.com

S. Author
second address

short term. Accordingly, the goal of DM1 treatment is to tightly control the blood glucose to levels as close to normal as possible without inducing hypoglycemia.

Manual treatment is cumbersome and error-prone because the insulin needs change over time due to physiological variation and external perturbations [1]. This necessitates lifelong precautions and permanent awareness of the disease, a burden that may significantly affect the quality of life [2]. Worldwide, researchers therefore aim to develop an artificial pancreas (AP), a fully automated system for glucose control [3]. The absence of permanent human supervision requires particularly reliable and safe systems [4], with safety defined as the absence of unacceptable risk [5]. A risk in this regard can originate from anything that compromises the intended functionality of the system and causes harm [6]. Standards on system safety engineering (e.g. IEC 61508) require that risks are reduced by safety functions designed to detect, notify and act upon faulty conditions [7].

This paper, therefore, performs a risk analysis of the safety-critical system from the perspective of the controller unit with an undefined control algorithm. The main motivation behind this paper is to (i) identify control challenges and risks associated with a fully automated AP which the controller needs to handle, and (ii) to suggest strategies to ensure a safe design of the control system. The second goal includes a recommendation whether the system should automatically respond or alert the user.

Following this introduction, the background of closed-loop glucose control and the safety of artificial pancreas systems is outlined in section 2. Section 3 contains the risk analysis beginning with the definition of the aim in section 3.1. The analyzed system and underlying assumptions are outlined in section 3.2, before the main hazards are deduced in section 3.3. Section 3.4 presents the actual risk analysis by means of Failure Modes and Effects Analysis. Section 4 and 5 summarize methods for fault and meal detection, respectively. Section 6 discusses different aspects of the results. Eventually, the work is concluded in section 7.

2 Background

In manual therapy of DM1, long-acting insulin is injected subcutaneously one or two times daily. Additional boluses of fast-acting insulin are injected immediately before meals to mitigate postprandial hyperglycemia. The glucose-elevating effect of each meal must be estimated in order to dose these pre-meal insulin boluses. The BGL is typically monitored by frequent capillary blood glucose measurements which are achieved by pricks into the fingertip. Devices for continuous glucose monitoring (CGM) in the subcutaneous (SC) tissue provide the glucose trend and can be used to take more informed therapeutic decisions. However, the readings of the common amperometric, enzyme-based sensors for SC can be substantially compromised by sensor drift, calibration errors and the physiological delay between blood and interstitial glucose concentration [8].

A more advanced option to administer insulin are insulin pumps that deliver fast-acting insulin continuously into the SC tissue. The basal insulin infusion rate (IIR) is adjusted throughout the day according to a manually pre-programmed protocol. These insulin pumps can be augmented by SC CGM. The state-of-the-art, *semi-automated* systems adjust the basal IIR automatically based on the CGM

readings. However, prandial insulin boluses still need to be initiated by the patient [9].

All insulin pumps on the market alert to low battery status and to an empty or nearly empty insulin reservoir [10]. The pumps also feature alarms to indicate an occluded delivery tube based on pressure and current measurements [10], but the detection is rather delayed dependent on the infusion rate and the length of the tubing [11,12]. Some modern pumps carry out automated safety functions based on SC glucose measurements (G_{SC}). If the glucose level drops below a threshold, an alarm is raised and the insulin delivery is suspended for a limited period ("low glucose suspend"). Novel pumps even include predictive pump shut-off algorithms that stop insulin delivery if a glucose level below the threshold is expected in the near future ("predictive low glucose suspend"). Several clinical studies give evidence for a certain benefit of such low glucose suspend systems in avoiding severe hypoglycemic events [13,14]. Nevertheless, they are to some extent unreliable with today's technology because erroneously low sensor readings often occur during night and can trigger pump shut-offs with resulting hyperglycemia [15]. These spurious activations of safety functions compromise the achievable performance of closed-loop glucose control. The extended time spent in hyperglycemia during studies with threshold suspend systems [13] may be explained by this.

Alerts and alarms inform about undesired or dangerous events and involve humans in the decision process. Such alarms affect not only the person with DM1 but also persons in the environment, in particular family members. The reasons, timing and sound level of alarms and alerts and their consequences are complex [16]. A high frequency of alarms may provoke alarm fatigue [17]. Today's sensor-augmented insulin pumps already alert to as many as 47 different events and conditions, with expected increasing numbers as the degree of automation further increases [16]. Thus, the decision between alarming the user and autonomous event handling is essential.

Existing *semi-automated* glucose control systems and concepts rely on manual user input to correct for meals or exercise. Experience indicates that self-monitoring is challenging [18] and such input often results in erroneous operation [19]. The ultimate goal is therefore to develop a *fully automated* AP which must autonomously give correct insulin doses, while detecting and coping with perturbations [20,21]. An equally important requirement is that the system suspends itself in a safe way in situations where a trustworthy control is not guaranteed.

Main control strategies are to some extent inherently robust and/or include safety functions. Integral windup protection in proportional-integral-derivative controllers, for example, has the potential to suspend insulin infusion when hypoglycemia is impending [22]; and it is relatively easy to use safety constraints to limit the insulin-on-board amount in model predictive control [23]. However, an overall safe system design requires that faults are handled by dedicated safety functions [7]. It is particularly challenging to identify the type of a single perturbation from the multiplicity of possible disturbances and faults. The diagnosis becomes even more complex when multiple faults are present simultaneously; for example, an erroneously low sensor signal while the insulin infusion suffers from an occlusion.

The risks of glucose control systems have been particularly analyzed in a few publications: The safety-related problems arising in an AP have been compared with those in air craft and the chemical process industry [24]. The risks associated with the software of insulin pumps have been outlined [10], whereas a hazard

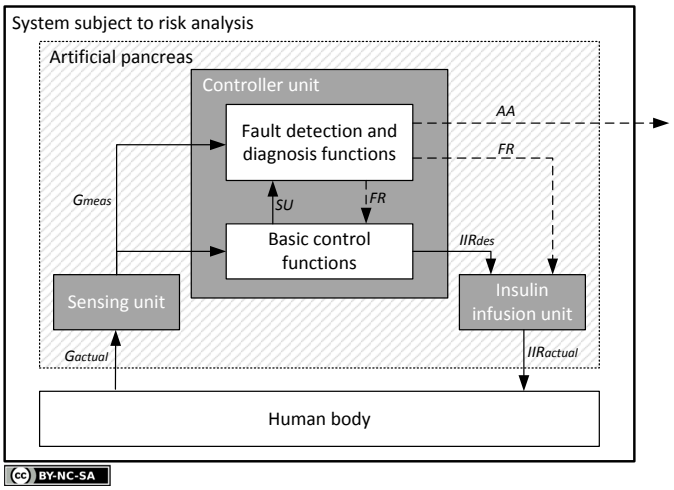

Fig. 1 Basic structure of single-hormone artificial pancreas with sensing unit, controller unit and insulin infusion unit. AA - Alarms, alerts (for external attention), FR - Fault response, $Gactual$ - Actual local glucose concentration, $Gmeas$ - Measured glucose concentration, $IIRactual$ - Actual insulin infusion rate, $IIRdes$ - Desired insulin infusion rate, SU - Set-up of basic control functions. The figure is licensed under a Creative Commons BY-NC-SA 4.0 license.

analysis including operation, software and hardware problems provides a more comprehensive overview [25]. Adverse events related to SC insulin infusion sets have been analyzed together with insulin pumps [26–29] or separately [30–32]. Furthermore, the importance of accurate glucose sensor signals and their processing has been discussed [33], as well as the variability of insulin sensitivity within and between subjects and the physiological factors [1,34]. Combining all this, a taxonomy of AP-related safety issues has been suggested [35]. Recently, safety aspects of the separate unit of an AP have been reviewed [36,37]. However, academic efforts to improve the safety of glucose control systems have mainly focused on the development of methods that react upon hypoglycemia rather than identifying strategies that act upon the root causes at the earliest possible time. The road map towards a *fully automated* AP, for example, contains steps that do not address specific faults but rather handle acute impending hypo- and hyperglycemia [38].

The present risk analysis starts at the origins by structurally analyzing perturbations with glycemic effect. The results shall support the development of reliable control algorithms and methods which maintain the system in a safe state despite all foreseeable and unforeseeable events. This includes appropriate reasoning and timing for user warnings.

3 Risk analysis

3.1 Aim

A typical single-hormone AP with three components, i.e. sensing unit, controller unit and insulin infusion unit, is analyzed. Figure 1 shows the analyzed system with

the human body as part of the control loop. Changes within the user's body affect the whole system and are therefore included in the risk analysis. The overall system is affected by both internal and external perturbations. Internal perturbations are faults within the system which impair the required performance, whereas external perturbations are unknown inputs acting on the system or its dynamics. The risk analysis is intended to serve as a basis to achieve an inherently safe design of the control system. In general, basic control functions can be differentiated from dedicated fault detection and diagnosis functions. The basic control functions deal with common disturbances under normal circumstances, whereas the fault detection and diagnosis functions respond to specific faults by either changing the basic control functions (e.g. adjusting the target BGL or minimizing the insulin infusion rate) or alerting the user. In addition, they may act as emergency barriers and override the basic control functions. The risk analysis includes both kinds of perturbations (disturbances and faults) in order to specify requirements for the whole controller unit.

3.2 Assumptions about the analyzed system

3.2.1 General

The desired functionality of the AP can in principle be realized with various designs. Here, a partially implanted system is considered with only the tip of the insulin infusion set and the sensing elements being within the body. All other electronics, the common batteries for power supply, the insulin reservoir, and the pump mechanism are situated outside the body. In case of insulin infusion into the peritoneal cavity (I_{IP}) or intraperitoneal glucose sensing (G_{IP}), the peritoneal port is established by physicians before the responsibility is transferred to the user. Both intended use and reasonably foreseeable misuse during installation, normal operation and end-of-lifetime are considered as fault sources. However, faults caused by poor installation which become obvious during system start-up, e.g. air bubbles in the tubing, are excluded. Though the use of off-the-shelf components is assumed, no specific products are considered. Failures due to inappropriate processing of material during manufacturing are excluded. Thus, random hardware failures (e.g. holes in tubing) are not considered. However, consumables degrade faster than the insulin pump and need to be changed frequently. These hardware failures due to degradation mechanisms within the lifetime of the insulin pump are considered, as are systematic failures occurring during insertion, installation, change and calibration of equipment. It is assumed that the system function is paused during maintenance.

3.2.2 Controller unit

The risk analysis aims to define general requirements on safe control functions without choosing a specific control strategy. Nonspecific basic control functions working perfectly in nominal control are assumed, thereby excluding controller errors which depend on the control strategy such as MPC [39]. Moreover, it is assumed in the analysis that no safety functions such as low-glucose-suspend systems

are implemented, though they became a standard in marketed insulin pumps. Safety functions in this context constitute functions for fault detection and diagnosis plus the necessary interface with basic control functions and the insulin infusion unit to ensure a specified response to detected faults. Neither meals nor exercises are announced to the controller unit whose application program may be integrated in the pump as in today's devices or run externally.

Firmware faults (e.g. timing or memory errors) are no particular property of the AP but may be present in any medical device software. The same holds for hardware failures of off-the-shelf electronic components. At this stage, neither firmware nor hardware faults are considered.

3.2.3 Insulin infusion unit

The insulin infusion unit consists of a traditional insulin pump including an insulin reservoir, and the insulin infusion set. Malfunction appears in any common, commercially available insulin pump [40]. However, here it is assumed that the insulin infusion pump works with specified accuracy and has no defects, failures of the insulin pump are not considered – the insulin pump works perfectly within its lifetime. The insulin infusion set typically consists of off-the-shelf plastic tubing, a steel needle or Teflon cannula as well as the connectors between pump and tube, and tube and needle/cannula [31]. Novel patch pumps contain the insulin infusion set and avoid thus incidents associated with the tubing [41] but are, however, not considered here. Fast-acting insulin is administered into abdominal SC tissue or into the peritoneal cavity. A port similar to DiaPort from Roche Diagnostics (Mannheim, Germany) [42] is assumed for I_{IP}. The insulin is administered with defined chemical and physical properties, i.e. no deterioration and no volume changes or formation of air bubbles due to ambient temperature or pressure changes.

3.2.4 Human body

By including the insulin-glucose physiology of the human body as a potential source of perturbations, a net nominal effect of insulin on the BGL can be assumed. All deviations from this nominal insulin-to-glucose net effect are treated as faults in the FMEA, regardless their origins. This corresponds to plant faults in the chemical process industry which change the dynamical input/output properties of the system [43]. Although the final control system will probably handle some altered dynamics as disturbances, referring to them as faults provides a structured and more comprehensive analysis. Moreover, they may impair the fault detection and therefore have to be considered while tuning the latter.

3.2.5 Sensing unit

The glucose concentration is continuously monitored by means of G_{SC} or G_{IP}. Within the sensing unit, the raw sensor signal is processed and transformed into a value for the glucose concentration at the sensing site. Common enzyme-based amperometric CGM technology is assumed for G_{SC} because of its widespread and dominant use. No specific technology has been established for G_{IP}. Besides erroneous sensor signals, communication loss caused by an unintended disturbance of

the often wireless transmission to the controller unit is included. Other communication issues such as the security of the signal transmission, i.e. the protection against intended incidents and privacy concerns, are out of the scope of this risk analysis.

3.3 Main hazards

The term hazard is used in this study as the potential source of injury or damage to the health of the AP user with DM1. Obviously, hyper- and hypoglycemia are hazardous situations because death or serious injuries can follow. The faults causing these undesired events are underdosing and overdosing of insulin, respectively. In addition, some faults may result in undefined dysglycemia as they disturb the given or required insulin doses in an undefined manner depending among other factors on properties of the AP (e.g. consequences of power loss).

3.4 Failure modes and effects analysis (FMEA)

The application of risk management to medical devices is subject of the international standard ISO 14971 [5]. The standard refers among others to *Failure Modes and Effects Analysis (FMEA)* as a standard technique for risk analysis. An FMEA provides extensive and structured information about faults and therefore builds a good basis for refinement of safety functions [73]. *Fault modes* rather than *failure modes* are actually analyzed in an FMEA, but the term failure modes and effects analysis is the common name of this methodology [7] and used in the resulting Table 1. The analysis was carried out by the authors with expertise in control and safety engineering, (medical) cybernetics, sensor technology, endocrinology, and medical care for patients with DM1. A preliminary version of the FMEA was presented as poster at ATTD 2016 [74].

The FMEA scheme in Table 1 was modified to fit the purpose of identifying the requirements for a fully automated safe AP control system. A brief description of the three analyzed units is given in the first column, followed by related faults that cause inappropriate dosing and therefore influence the glycemic status. An extensive literature study gathered the listed faults, which were chosen and sorted based on the expected disturbing effect on the controller performance, i.e. the glycemic control. Long-standing experience in the treatment of DM1 from the perspective of both physicians and patients supported the selection process. The analysis focuses on systematic faults that occur deterministically under given conditions caused by hardware or human actions according to the classification in annex B of ISO/TR 12489:2013 [75], whereas systematic firmware faults and random hardware faults have been excluded. The degradation of enzymatic sensors is considered as systematic hardware failure as the rate is mainly affected by sensor design and specification. The faults are further detailed by fault modes, causes and typical circumstances of occurrence. Particularly fault prone technologies or sensing and infusion routes, respectively, are stated to emphasize the differences between the SC and the IP approach.

In addition, fault appearance characteristics are classified into incipient, intermittent and abrupt based on standard literature on fault diagnosis [4]. Abrupt

Table 1. Failure Modes and Effects Analysis of an Artificial Pancreas.

Description of unit	Description of failure				Risk evaluation (SC/IP)			Risk reduction		
	Failure mode	Failure cause	Circumstances/ Operation mode of occurrence	Appearance characteristics [13, p.63]	Occur-rence O	Seve-rity S	Risk priority number	Automated detection by limit checking on CGM and IIR data	Control system's response to detected failure	Additional mitigating measure
Sensing unit and sensing site • Measures glucose concentration at sensing site • Determines BGL based on that	Positively biased signal	Miscalibration	Calibration during changing BGL [44]; particularly SC (physiological time lag)	3	5	4	60	Positive/negative BGL' exceeds stable-level threshold during calibration.	Request to repeat calibration; set IIR to basal; stop infusion if not calibrated within certain period.	Refine calibration procedure. Sensor redundancy.
			Too infrequent calibration (drift due to degrading enzymatic sensor components) [44]	1	5	3	15	Defined time since calibration exceeded.	Request calibration; set IIR to basal; stop infusion if not calibrated within certain period.	Alternative sensing technology.
			Calibration at low values during fluctuating local glucose after long-term SC implantation [45]	3	5	4	60	Defined time since sensor change exceeded.	Request sensor change; set IIR to basal; stop infusion if not changed within certain period.	Alternative sensing technology.
		Interference with other analytes	Presence of other metabolites e.g. sugars [44], medication with e.g. acetaminophen [47]; optical sensors [44]	3	3	4	36	Not covered by automated detection.	Request manual treatment; stop infusion.	Perm-selective coating [44]. Alternative sensing technology.
	Negatively biased signal	Loss of sensitivity to glucose	Pressure induced sensor attenuation during night or due to tight clothing [48]	3	7/3	2	42/18	Sudden negative drop of BGL. More advanced methods (section 4).	Set IIR to basal; stop infusion if BGL does not recover within certain period.	Continuous sensor impedance monitoring. Sensor redundancy. Alternative sensing route. Use predicted BGL to calculate IIR.
			Isolated unphysiological spikes caused by user's motion [48]	3	5/3	2	30/18	BGL' exceeds physiological thresholds for a short period. More advanced methods (section 4).	Ignore affected samples; set IIR to basal if lasting longer than a few samples.	Sensor redundancy. Use predicted BGL for calculation of IIR.
			Incomplete SC insertion or dislocation (signal averaging over whole length)	3	3-5/1	3	45/9	Not covered by automated detection.	Request sensor change; set IIR to basal; stop infusion if not changed within certain period.	Continuous sensor impedance monitoring. Sensor redundancy. Use predicted BGL to calculate IIR.
		Lowered local glucose concentration	Bleeding caused by insertion into SC tissue [50]	1	3-5/2	3.5	17.5/7	Not covered by automated detection.	Request sensor change; set IIR to basal; stop infusion if not changed within certain period.	Continuous sensor impedance monitoring.
			FBR, local fibrous tissue after years of sensing in same SC area [51]	1	3-5/NA	3	15/NA	Not covered by automated detection.	Request sensor change.	Alternative sensing route.
			Bleeding caused by sensor dislocation during physical activity [50]	1	4-5/1	3.5	17.5/3.5	Not covered by automated detection.	Request sensor change; set IIR to basal; stop infusion if not changed within certain period. Stop infusion until blood clot disappears [50].	Alternative sensing route.
			Sensor enclosed by peritoneal wall prohibiting glucose diffusion	3	NA/4	3.5	NA/42	Not covered by automated detection.	Request sensor relocation.	Alternative sensing route. Sensor redundancy.
			Sensing too close to insulin infusion	1	4	4	16	I/G change exceeds physiological threshold.	Request sensor change.	Refine insertion equipment and procedure.
		Miscalibration	Calibration during changing BGL [44]; particularly SC (physiological time lag)	3	5/3	4	60/36	Positive/negative BGL' exceeds stable-level threshold during calibration.	Request to repeat calibration; set IIR to basal; stop infusion if not calibrated within certain period.	Refine calibration procedure. Sensor redundancy.
			Too infrequent calibration (drift due to degrading enzymatic sensor components) [44]	1	5	3	15	Defined time since calibration exceeded.	Request calibration; set IIR to basal; stop infusion if not calibrated within certain period.	Alternative sensing technology. Alternative sensing route.
		Sensor degradation	Biofouling-induced degradation of enzymatic sensors in SC tissue [44]	1	5	3	15	Defined time since sensor change exceeded.	Request sensor change; set IIR to basal; stop infusion if not changed within certain period.	Alternative sensing technology. Alternative sensing route.
	Delayed signal	Slowed diffusion	Fibrosis after long-term SC use [51]	1	5/4	3/2	15/8	Not covered by automated detection.	Request sensor change. Decrease calculated IIR by a safety factor.	Alternative sensing route. Sensor redundancy.
		Bio-contamination	Inappropriate sensor insertion into peritoneal cavity	1	3/4	3	9/12	Not covered by automated detection.	Request sensor change; set IIR to basal; stop infusion if not changed within certain period.	Alternative sensing route. Sensor redundancy.
	No signal	Communication loss	Shielding, too long distance for wireless transmission	3	5	3	45	No value.	Set IIR to basal; stop infusion if not re-established within predefined period and alert.	Refine equipment.

Table 1 - continued. Failure Modes and Effects Analysis of an Artificial Pancreas.

Insulin infusion unit and infusion site • Delivers insulin according to insulin infusion rate received from control unit • Absorbs delivered insulin	Under-delivery	Empty reservoir [25]	Not refilled on time	5	5	2	50	Logged amount of delivered insulin exceeds reservoir volume. BGL exceeds hyper-glycemic threshold. More advanced methods (section 4).	Stop infusion; request reservoir replacement.	Early refill reminder based on logged amount.
		Air bubbles	During installation, ambient tem-perature or pressure change [52]	3	5	1	15	Not covered by automated detection.	Increase IIR accordingly (not relevant for (most) adult users).	Refine equipment.
		Leakage due to disconnection of infusion set [25]	Intentional disconnection without announcement	5	4	2	40	BGL exceeds hyperglycemic threshold. More advanced methods (section 4).	Stop infusion; request visual check.	Pressure sensor.
			Inadvertent disconnection without user being aware	5	4	3	60	BGL exceeds hyperglycemic threshold. More advanced methods (section 4).	Stop infusion; request visual check.	Refine equipment. Pressure sensor.
			Connectors not properly closed after infusion set change	5	5	3	75	BGL exceeds hyperglycemic threshold. More advanced methods (section 4).	Stop infusion; request visual check.	Refine equipment. Pressure sensor.
		Occlusion [11]	Chemical precipitation	5	5	3	75	BGL exceeds hyperglycemic threshold. More advanced methods (section 4).	Stop infusion; request infusion set change.	Infusion set change after 3 days [54]. Refine equipment (shorter tube [11]; side port [53]). Pressure sensor. Larger microboluses. Alternative infusion route.
		Infusion set kinked [55]	Caused by patient movements or during insertion; particurlarly Teflon cannula [31]	4	7	3	84	BGL exceeds hyperglycemic threshold. More advanced methods (section 4).	Stop infusion; request infusion set change.	Replace steel needle by Teflon catheter [30].
		Leakage out of body through transdermal/-abdominal tunneling	Leakage from infusion site (swollen/contorted skin) [30]	1	3	3	9	BGL exceeds hyperglycemic threshold. More advanced methods (section 4).	Stop infusion; request infusion set change.	Replace steel needle by Teflon catheter [56].
			Accidental catheter dislocation [55]; in SC tissue, particularly Teflon cannulas [31]	5	4/3	3	60/45	BGL exceeds hyperglycemic threshold. More advanced methods (section 4).	Stop infusion; request infusion set change.	Replace steel needle by Teflon catheter. Alternative infusion route.
			Incomplete insertion	5	4/2	2	40/20	BGL exceeds hyperglycemic threshold. More advanced methods (section 4).	Stop infusion; request infusion set change.	Refine port design and insertion procedure.
		FBR	Long-term foreign objects inside the body; changed insulin absorption; particularly Teflon cannulas in SC tissue	1	5/4	2	10/8	BGL exceeds hyperglycemic threshold. I/G change exceeds physiological threshold.	Increase IIR; request infusion site change.	Steel needle instead of Teflon catheter. Alternative infusion route.
		Lipodystrophy [57]	Long-term insulin administration into same SC area	1	4	2	8	BGL exceeds hyperglycemic threshold. I/G change exceeds expected threshold.	Request infusion set change [57].	Alternative infusion route.
		Tip of cannula blocked	Cannula sticks in peritoneal wall or is blocked by FBR	2	5	2	20	BGL exceeds hyperglycemic threshold.	Request catheter relocation.	Pressure sensor.

Table 1 - continued. Failure Modes and Effects Analysis of an Artificial Pancreas.

Human body • Receives insulin from insulin infusion unit • Lowers glucose concentration according to I/G	Decreased I/G	Decreased insulin sensitivity	Weight gain [1]	1	3	2	6	Prolonged, slightly increased average BGL.	Increase IIR.	Adapt control law [1].
			Medication [1],[58]	3	3	2	18	Increased average BGL.	Increase IIR.	Adapt control law [1].
			Illness, medical and surgical stress [1],[58]	3	4	3	36	Increased average BGL.	Increase IIR.	Adapt control law [1].
			Mental stress (net effect) [1],[58],[59]	3	5	3	45	Increased average BGL.	Increase IIR.	Adapt control law [1]. Measure galvanic skin response, heart rate sensor [60].
		Increased hepatic glucose production	Prolonged high BGL due to hypoinsulinization (results in dawn phenomenon) [34]; safety margins of SC infusion	1	6/4	3	18/12	Prolonged increased average BGL.	Increase IIR.	Physiologically tight target range [34].
		Oral glucose consumption	Meal with specific macronutrient composition [1]	5	7	2	70	One or a combination of BGL, BGL', BGL'' - based on raw data or KF - exceeds positive thresholds within a certain time window [61,62,63]. More advanced methods (section 5).	Increase IIR.	Adapt control law [1]. Anticipatory control based on meal prior probabilities [66.67].
	Increased I/G	Increased insulin sensitivity	Long-term physical training program [1]	1	3	2	6	Prolonged decreased average BGL.	Decrease IIR.	Adapt control law [1].
			Previous physical activity affecting SI [34]	3	5	3	45	Temporary decreased average BGL.	Decrease IIR.	Adapt control law [1].
			Acute physical activity, aerobic vs. anaerobic [68,69]	4	5	4	80	BGL' exceeds negative threshold.	Decrease IIR. Request rescue food.	Include data from activity tracker and/or physiological parameters [70].
			Weight loss [1]	1	3	2	6	Prolonged, slightly decreased average BGL.	Decrease IIR.	Adapt control law [1].
			Glucose lowering medication [24]	3	4	4	48	Decreased average BGL.	Decrease IIR.	Adapt control law [1].
			Meals (net improved SI) [34]	3	7	1	21	Decreased average BGL.	Decrease IIR.	Adapt control law [1].
		Inhibited gluconeogenesis	Alcohol (increased hepatic SI, normal peripheral SI) [1]	1	5	4	20	Temporary decreased average BGL.	Decrease IIR.	Adapt control law [1].
		Decreased hepatic glucose production	Prolonged low BGL due to hyperinsulinization [34]; slow dynamics of SC infusion	1	6	4	24	Prolonged decreased average BGL.	Decrease IIR.	Physiologically tight target range [34].
	Undefined cyclic changes of I/G	Circadian rhythm	Diurnal metabolic state [34], [71]	3	6	3	54	Varied average BGL.	In-/decrease IIR.	Adapt control law [1].
		Irregular sleeping patterns	Weekdays vs. weekends, shift work [1]	3	5	3	45	Varied average BGL.	In-/decrease IIR.	Adapt control law [1]. Activity monitor [72].
		Menstrual cycle [1]	Only relevant for female users in a certain period of age.	3	4	3	36	Varied average BGL.	In-/decrease IIR.	Adapt control law [1].
	Undefined one-time change of I/G	Puberty [1]	Typical age	2	2	4	16	Varied average BGL.	In-/decrease IIR.	Adapt control law [1].
		Menopause [1]	Typical age	2	2	4	16	Varied average BGL.	In-/decrease IIR.	Adapt control law [1].
		Pregnancy [1]	Only relevant for female users; depends on trimester	2	2	4	16	Varied average BGL.	In-/decrease IIR.	Adapt control law [1].
		Biocontamination (local inflammation)	Insterile equipment or inappropriate handling during particularly IP insertion	1	1	4	4	Varied average BGL.	Request sensor and infusion set change.	Refine port design and insertion procedure.

BGL - blood glucose level, BGL' - first time derivative of BGL, BGL'' - second time derivative of BGL, FBR - foreign body response, IIR - insulin infusion rate, IP - intraperitoneal//*G* - insulin-to-glucose net effect, KF - Kalman filter, SC - subcutaneous, SC - subcutaneous, SI - insulin sensitivity, UKF - Unscented Kalman filter

Fault appearance characteristics: 1 Incipient, 2 Intermittent/Incipient, 3 Intermittent, 4 Abrupt/Intermittent or Abrupt/Incipient, 5 Abrupt.

Risk evaluation. Likelihood of occurrence: 1 < Once in a lifetime, 2 Once in a lifetime, 3 Once a year, 4 Once a month, 5 Once a week, 6 Once a day, 7> Once a day, NA Not applicable.

Severity: 1 Light or negligible hyperglycaemia, 2 Moderate hyperglycaemia or light hypoglycaemia, 3 Severe hyperglycaemia or moderate hypoglycaemia, 4 Diabetic ketoacidosis (DKA) or severe hypoglycaemia

faults are characterized by a sudden and complete loss of function for the affected unit, whereas intermittent faults cause an irregular and time-limited loss of function. Faults leading to a drift in performance, that may eventually result in a complete loss of function if not corrected, are categorized as incipient. The function of each unit is defined in the description of the unit. A numerical value is assigned to all appearance categories for the purpose of risk ranking. An abrupt fault appearance is ranked worst (5) because the unit looses its function without prior signs and thus without the possibility for detection. An incipient behavior, on the other hand, is ranked least critical (1) since the deviation might be detected before the function is completely lost. An intermittent behavior (3) is considered to be less disastrous than an abrupt fault because the controller can regulate the BGL normally between the periods with lost function. The impact of the duration of the function loss is neglected.

The qualitative risk evaluation comprises (i) the likelihood of occurrence, and (ii) the severity of each fault. In the absence of sufficient publicly accessible data, both were judged by the authors based on own experience and indications from literature. An integer between 1 and 7 indicates the likelihood of occurrence for the single user as incidences per time, ranging from *less than once in a lifetime* (1) to *several times a day* (7). How likely a particular fault occurs may significantly vary for different patients; thus a range is given for some faults which can be read as *'from ... to ...'*. If a particular fault is not applicable to the SC or IP approach, this is indicated by *NA* in the occurrence category. The severity of a fault is ranked according to categories which can be interpreted as the harm that threatens the user. Four categories are distinguished with *Light or negligible hyperglycemia* being the least severe (1) and *Diabetic ketoacidosis or severe hypoglycemia* the severest category (4).

Higher numbers indicate a higher risk for the specific fault. The appearance characteristics, the likelihood of occurrence and the severity are combined in a risk priority number (RPN) by multiplying the single numbers. A fault with high RPN is most crucial in system design, whereas a low RPN indicates a less critical fault. For those faults where likelihood was defined as a range, the highest likelihood was used to calculate the RPN.

The last part in Table 1 deals with possibilities to reduce the risk of faults. Methods for automated fault detection are reported first. Automated detection means that the system detects this specific fault automatically based on sensor information without human interaction. In accordance with the goal of the analysis, only methods based on data that is available in a minimally sensor-equipped AP, i.e. glucose measurements from CGM and IIR data as well as time, are included. In Table 1, fault detection by means of limit checking is reported, whereas "More advanced methods." refers to more advanced detection methods that are summarized in section 4. Limit checking is based on the assumption that absolute values or trends of monitored variables violate a threshold caused by a single specific fault while the rest of the system remains in faultless condition.

The appropriate automated response to detected faults is subject of the next column. Some fault causes cannot be eliminated by an automated action, but rather request the user to intervene by changing the sensor or the insulin infusion set. The decision between handling the fault autonomously or informing the user is specified as fault response. Some perturbations, in particular physiological changes, should be addressed by adjusting the insulin infusion rate automatically. The

adjustments to mitigate an increased insulin sensitivity caused by previous physical activity, for example, should be within the nominal range of the basic control functions. The effect of a long-term physical training program, on the other hand, might be best considered by a permanent adaptation of the control law. An explicit detection and differentiation from other perturbations may not be reasonable or even possible for all physiological changes. They could instead be lumped into a common changed physiology. However, the fault causes are listed separately because one must ensure to reasonably consider each of them when designing the control system.

Additional measures for risk reduction and mitigation are suggested, including an adaptable controller design and additional sensors which have been previously excluded. Training or a diet restriction are not listed as methods of risk reduction because this analysis focuses on measures that can be implemented with the controller design or by hardware refinement, though an appropriate behavior of the user may significantly reduce the risk in some cases.

The measures for risk reduction are not meant as additional safety layers which are only active when the control function fails but should always be implemented building the normal control system.

4 Detection of sensor and insulin infusion faults

Successful fault detection and diagnosis can provide the possibility to differentiate between situations that can be handled autonomously and those in which the user must be alerted.

Among the sensor faults, the fault modes *isolated spike* and *transient negative bias* were addressed particularly often. Both fault modes are considered as intermittent faults in Table 1. Isolated spikes are inherently random signal abnormalities rather than permanent sensor failures. The negatively biased sensor signal is assumed to be transient because its major given cause is lost sensitivity due to pressure induced sensor attenuation (PISA) during night. Zhao and Fu (2015) [49] used steps to model isolated spikes and a biased signal. Generic signal anomalies (positive and negative steps, exponential changes and drift, and random noise) were analyzed for fault detection [76,77]. Although those anomalies cannot be directly related to particular faults, they build a comprehensive basis for signal fault modeling in simulation studies. Instead of the actual kind of CGM fault, it was also investigated whether the sensor readings are correct or incorrect [78–81].

The studied fault modes of the insulin infusion unit are *no delivery*, *under-delivery* and *over-delivery*. Infusion set failures can be detected either directly or indirectly [15]. Direct detection builds upon the signals of sensors integrated in the pump. This is realized to detect occlusions in marketed insulin pumps by force sensors and ammeters [10]. Most methods aim to detect faults indirectly based on either tremendous BGL excursions or a changed glucose lowering effect of insulin [82]. Although different faults are claimed to cause no delivery and under-delivery, i.e. disconnection [15,83], leakage [83], and complete [48] or partial occlusion [84–88], the fault causes were usually not further examined after detection. Since the user must change (parts of) the insulin infusion unit upon these faults, one might not see the advance of a further diagnosis [89]. However, a more detailed fault evaluation could help the user to identify the particular problem.

The number of publications on fault detection is surprisingly low compared with the number of publications on algorithms for closed-loop glucose control. A categorized overview of the methods proposed for fault detection in glucose control has been presented recently [90].

5 Detection of meals

Besides acute physical activity, meals are one of the major physiological perturbations that the glucose controller has to handle. This is represented by the high RPN in Table 1. Worldwide research efforts led to significant achievements in closed-loop glucose regulation but the postprandial period remains a challenge. The control algorithms that are tested in clinical studies often require meal announcements by the user.

Automated meal detection has received increasing attention during the past years. The earlier methods detect a meal based on threshold violations of (occasionally filtered) CGM values. Recently, more complex methods using a model of the glucose-insulin metabolism and data-driven methods were proposed. Most approaches for meal detection utilize the measurements of one CGM device.

Meal detection by threshold checking has been suggested with different combinations of checked variables; the raw CGM data is either directly used or revised by removing measurement noise using a linear noise model in a Kalman filter (KF) [61,91,62]. Alternatively, the nonlinear Bergman minimal model has been used to estimate the rate of glucose appearance in plasma with an unscented KF (UKF), and meals were detected when this estimate exceeded an upper threshold [21,92].

Several model-based methods exploit versions of the minimal model by Bergman. Two redundant glucose sensors were used in a set-up to detect both faults and meals [93]: An UKF is separately applied to the two sensor signals to predict multiple steps of the CGM values. Based on a statistical comparison of the covariance matrices of these two predictions, a meal or fault is detected. Moreover, it was proposed to detect a meal if the cross-correlation between two states (the SC glucose concentration and a lumped state) estimated by an UKF exceeds a threshold [94,95]. An augmented version of the Bergman model was also used in a method that applies invariant statistics to differentiate between effects that can be explained by the model with previously detected meals as input and those that must result from a more recent meal [96]. Another approach applies linear discriminant analysis to state horizons that were generated by moving horizon estimation using a version of the Bergman minimal model [97].

Besides the estimator-based methods with an underlying model of the glucose-insulin metabolism, data-driven methods have been proposed as well. Fuzzy logic was used to categorize segments of CGM data according to their shape [98,99].

6 Discussion

6.1 Most critical faults

Functional safety is achieved if the risk is as low as reasonably practicable [7]. A high RPN indicates particularly safety-critical faults, either because of high li-

kelihood of occurrence, high severity, abrupt appearance or a combination of all. The higher the RPN, the greater is the need for risk reduction by measures as those suggested in Table 1. Faults with high RPN are not tolerable; risk reducing measures must be implemented and their success must be verified by recalculating the RPN to ensure that the remaining risk is acceptably low. Faults with medium RPN may be tolerable only if risk reducing measures are implemented, thereby lowering the risk and increasing the comfort for the patient. Faults with very low RPN may even be accepted without risk reducing measures. The calibration routines need special attention with respect to the performance of the sensing unit. Problems with the insulin infusion set, i.e. kinking, occlusion, disconnection or dislocation, were identified as most critical in the insulin infusion unit. The highest RPN for changed dynamics within the human body was deduced for acute physical activity. Together with meals, exercise is the most challenging perturbation. The perturbations within the human body that can be corrected by automated IIR adjustment are rather disturbances than faults. The basic control functions should either be robust to these or adapt to long-lasting altered dynamics. The fault appearance characteristics can be adduced to decide whether robustness or adaptation is the better solution in each case. An incipient time behavior implies adaptation, whereas an abrupt behavior prompts robustness.

6.2 Scope and limitation of the study

6.2.1 Significance of the analyzed system

In this study, we have studied a general system on the basis of the required functional capacity of each of the system elements. Faults have been identified by investigating the possible technical causes, and causes that may stem from complex and sometimes ambiguous phenomena of the human body. That fulfills the goal to develop an overview of high-level requirements for a safe control system. However, a more specific risk analysis is needed to successfully design the controller unit of a specific system. Research groups might have done similar analyzes as preparation for clinical trials but did not publish them.

Controller faults such as numerical problems were excluded because the main purpose of this risk analysis is to identify the physiological conditions and failure scenarios outside the controller, which the controller needs to handle. After the control strategy has been defined based on the deduced safety requirements, a risk analysis should be performed that considers specific limitations of the controller, given its actual implementation. Some faults, such as a kinked insulin infusion set, can be avoided by adequate equipment handling and behavior of the patients. However, the system design must also consider the potential occurrence of these faults whose likelihood of occurrence can be reduced by educating the patients. It was omitted to list the patient education as mitigating measure because this is not an automated system response.

Over-delivery of insulin caused by faults in the insulin infusion unit might occur due to faulty mechanical parts, but are unlikely in normal operation with functioning equipment. Thus, the related failure modes were out of the scope of this analysis. Over-delivery of insulin could also be caused by controller faults which were also excluded as mentioned above. The asymmetrically higher risk of over-

delivery (hypoglycemia) compared with under-delivery (hyperglycemia), however, suggests to prioritize detecting the former. Besides an overall conservative insulin dosing to prevent over-delivery, bi-hormonal AP systems provide the opportunity to inject glucagon as an effective mitigating measure.

6.2.2 Limited publicly accessible data on faults

The FMEA scheme in Table 1 contains a list of potential faults of an AP gathered by literature study. A quantitative risk evaluation using historical data was, however, not performed due to the lack of quantitative information about fault frequencies and severity. Unannounced changes and improvements of equipment frequently invalidate published data for newer versions [26]. An international central register of adverse events related to faults of medical devices, e.g. in glucose control systems, could provide valuable information not only for users and health care providers but also for persons engaged in the development and improvement of such devices [6]. The existing databases in Europe (European Databank on Medical Devices (EUDAMED)) and the USA (Manufacturer and User Facility Device Experience (MAUDE)) are a starting point for adequate surveillance after the launching of medical devices but but their present form and procedures can be improved [100].

Moreover, close to no experience has been gained with G_{IP} due to the absence of appropriate sensing technology. The evaluation of this approach requires experimental data.

6.2.3 Risk acceptance criteria

A risk analysis gains value by judging the identified risks on risk acceptance criteria. The need for mitigating measures and their success is quantified based on risk acceptance criteria [5]. Generic descriptive safety requirements for insulin pumps have previously been suggested [101]. Such internationally obligatory criteria could help improving the safety of the AP. Quantitative risk acceptance criteria for medical devices are defined in each company based on organizational policies [102]. No risk acceptance criteria were applied here, though the RPN indicates the more critical faults. Without quantitative fault information (section 6.2.2), however, it is rather difficult to prioritize faults.

6.3 Safety by modularization

A modularized system structure is typical to safely manage various faults and has already been implemented in an AP [103]. Modularization according to the fault locations, e.g. sensor signal validation vs. insulin infusion surveillance, is one possibility. Furthermore, the time dependency of faults influences which detection method is appropriate [4] and motivates fault detection and diagnosis functions working on different time scales. The combination of different detection methods is most promising in this context [104].

After having detected the occurrence of a fault, the system can either inform the basic control or issue an alert (AA in Fig. 1). However, the user might ignore major incidents when the alarm frequently goes off for minor reasons. To

avoid this alarm fatigue, it is important to identify the fault causes as precisely as possible and to decide whether the user needs to be informed. The possibility of multiple faults and changes in the insulin-glucose dynamics (Table 1) requires a balanced tradeoff between fault sensitivity and specificity. Even though a visual inspection might be unavoidable to eventually clarify the root cause of the fault, the controller can guide the user through a systematic search based on risk severity and the probabilities of possible faults. Its implementation, however, requires a comprehensive database with quantitative risk information (section 6.2).

All functions must be designed as part of the overall system. The example of a sensor signal that is discontinuous due to calibration shows the importance of system integration. An uninformed fault detection unit could easily mistake the step in the signal for a fault; including calibration information may reduce the number of false alerts in this case [105].

6.4 Redundancy as limited option for fault tolerance

Redundancy enhances the fault tolerance of technical systems notably because redundant identical or diverse components perform the functionality of faulty components [4]. Since a portable medical device for permanent use in daily life is supposed to be as small and inconspicuous as possible, redundant insulin pumps or infusion sets seem inappropriate. Static or dynamic redundancy of the controller unit may, however, be realized depending on the hardware configuration.

The sensor performance is particularly critical because it is the only input entering the AP and false sensor readings proceed through the other components. Sensor redundancy can compensate for drift and signal dropouts [106]. Only two SC sensors already improve the signal accuracy whereas voting schemes of three or four sensors are even more effective [106]. So-called orthogonal redundancy (or sensor fusion) combines different sensing technologies [107] which ideally do not suffer from the same disturbances. Combining the sensor modalities in a smart way, the resulting glucose estimate will have both higher accuracy and lower failure rate compared to each sensor type used alone. However, wearing multiple separate SC sensors attached to the body certainly impairs the experienced comfort [108]. Additional glucose signals can also be achieved by mathematical model simulation [43]. This so-called analytical redundancy can be used to confirm measurements and to replace faulty measurements as controller inputs.

6.5 Extending the pool of monitored data

The distinction between fault classes and even some single faults may be possible with a feature space based only on the commonly available CGM and IIR data. More valuable information, however, can be expected if more information about the state of the system is considered. The measured glucose concentration is, for example, not a good indicator of a sensor failure. A more suitable approach for fault detection is to utilize the internal state of the sensor gathered by monitoring data (e.g. impedance and noise current of amperometric sensors) [78, 79]. Several attempts have been made to incorporate additional bio-signals in the generation of hypo- and hyperglycemic alarms [109]. However, only a few methods on fault

detection in AP exploit information beyond monitored glucose values and the insulin infusion rate [90]. Body temperature and septic status, for example, describe the general health condition [80,81], whereas activity monitors provide information about the current life situation [72]. A human estimating the correct insulin dose considers all that. Automated diabetes management could also be improved by extending typical diabetes care data (i.e. CGM and IIR) with information that is already available from fitness devices and weighing scales, if only the connectivity of related devices would be standardized [18,110]. Statistical analysis of such data could, for example, enable to predict the glucose levels following the onset of physical activity across patients.

7 Conclusion

This work provides a failure mode and effects analysis for a glucose control system composed of common technologies, kept as general as possible. In particular, perturbations that potentially cause hypoglycemia or hyperglycemia are analyzed. The result is a structured overview of faults and disturbances that the controller unit has to handle.

Academic research towards an AP has neglected faults for the most part. Although some approaches exist to avoid hypoglycemic events in particular, the focus lies on impending hypoglycemia rather than on the fault causes. Along the same lines, methods on fault detection and diagnosis in the AP have focused on detecting single faults whereas the possible presence of other incidents is neglected. Since different perturbations may have a similar effect on the BGL, i.e. glucose lowering or increasing, fault diagnosis is essential. The diagnosis should reveal more information about an occurred fault than only its presence. At the best, the fault cause is identified which allows an appropriate system response. This detailed knowledge can also avoid alerting the user for minor reasons, and thus preventing alarm fatigue and increasing the overall acceptance of the AP. The present work provides an overview of perturbations, i.e. faults, disturbances and altered dynamics, with either direct or indirect metabolic effect. Criteria for designing and testing a robust and fault tolerant control system can be developed using this information. Some faults, such as a kinked insulin infusion set, may be avoided by adequate equipment handling and behavior by the patients. However, the system design must consider the potential occurrence of such faults.

Quantitative risk information about faults and their causes can improve the comprehensiveness of the risk analysis. Further contributions are needed in particular in identifying features to isolate faults, altered dynamics and external disturbances from each other. The inclusion of additional sensors supervising the physical system state and body monitoring data should be considered in this context.

Terminology

Adverse event	Any untoward medical occurrence, unintended disease or injury, or untoward clinical signs (...) in subjects, users or other persons, whether or not related to the investigational medical device [111]
Artificial pancreas	Closed-loop control of blood glucose in diabetes, is a system combining a glucose sensor, a control algorithm, and an insulin infusion device [112]
Disturbance	An unknown (or uncontrolled) input acting on a system [113]
Error	Discrepancy between a computed, observed or measured value or condition, and the true, specified or theoretically correct value or condition [114]
Failure	The termination of the ability of an item to perform a required function [114]
Failure mode	Manner in which failure occurs [114] (Fault modes rather than failure modes are actually analyzed in an FMEA, but the term failure modes and effects analysis is the common name of this methodology [7].)
Fault	Inability to perform as required, due to an internal state [114]
Fault detection	Event by which the presence of a fault becomes apparent [114]
Fault diagnosis	Action to identify and characterize the fault [114]
Fault identification	Determination of the size and time-variant behaviour of a fault. Follows fault isolation [113]
Fault isolation	Determination of the kind, location and time of detection of a fault. Follows fault detection [113]
Fault tolerance	Ability of an item to perform a required function in the presence of certain given sub-item faults [114]
Harm	Physical injury or damage to persons, property, and livestock [114]
Hazard	Potential source of harm [114]
Hazardous event	Event that can cause harm [114]
Hazardous situation	Circumstance in which persons, property and livestock or the environment are exposed to at least one hazard [114]
Intended use	Use of a product, process or service in accordance with the information for use provided by the supplier [114]
Perturbation	An input acting on a system, which results in a temporary departure from the current state [113]
Random hardware failure	Failure, occurring at a random time, which results from one or more of the possible degradation mechanisms in the hardware [115]
Reasonably foreseeable misuse	Use of a product, process or service in a way not intended by the supplier, but which may result from readily predictable human behaviour [114]
Residual	A fault indicator, based on a deviation between measurements and model-equation-based computations. [113]
Perturbation	An input acting on a system, which results in a temporary departure from the current state [113]
Risk	Combination of the probability of occurrence of harm and the severity of that harm [114]
Risk analysis	Systematic use of available information to identify hazards and to estimate the risk [114]
Reliability	Ability to perform as required, without failure, for a given time interval, under given conditions [114]
Safety	Freedom from unacceptable risk to the outside from the functional and physical units considered [114]
Systematic failure	Failure that consistently occurs under particular conditions of handling, storage or use [114]

References

1. Y. C. Kudva, R. E. Carter, C. Cobelli, R. Basu, and A. Basu, "Closed-loop artificial pancreas systems: physiological input to enhance next-generation devices," *Diabetes Care*, vol. 37, no. 5, pp. 1184–1190, 2014.
2. M. Debono and E. Cachia, "The impact of diabetes on psychological well being and quality of life. the role of patient education," *Psychology, Health & Medicine*, vol. 12, no. 5, pp. 545–555, 2007.
3. J. Kropff and J. H. DeVries, "Continuous glucose monitoring, future products, and update on worldwide artificial pancreas projects," *Diabetes Technology & Therapeutics*, vol. 18, no. S2, pp. S2–53–S2–63, 2016.
4. R. Isermann, *Fault-Diagnosis Systems: An Introduction from Fault Detection to Fault Tolerance*. Springer Berlin Heidelberg, 2006.
5. ISO 14971, *Medical devices - Application of risk management to medical devices*, ISO Standard, 2007.
6. G. Avendaño, "Critical importance of multilateral studies related with adverse events in medical devices," *Health and Technology*, vol. 6, no. 3, pp. 213–227, 2016.
7. M. Rausand, *Reliability of safety-critical systems : theory and application*. Wiley, 2014.
8. J. R. Castle, J. M. Engle, J. El Youssef, R. G. Massoud, and W. K. Ward, "Factors influencing the effectiveness of glucagon for preventing hypoglycemia," *J Diabetes Sci Technol*, vol. 4, no. 6, pp. 1305–1310, 2010.
9. Medtronic plc, *MiniMed®670G System User Guide*, Medtronic plc, 2017.
10. J. B. Welsh, S. Vargas, G. Williams, and S. Moberg, "Designing the modern pump: engineering aspects of continuous subcutaneous insulin infusion software," *Diabetes Technol Ther*, vol. 12, no. S1, pp. S37–S42, 2010.
11. A. C. van Bon, D. Dragt, and J. H. DeVries, "Significant time until catheter occlusion alerts in currently marketed insulin pumps at two basal rates," *Diabetes Technol Ther*, vol. 14, no. 5, pp. 447–448, 2012.
12. E. McVey, S. Keith, J. K. Herr, D. Sutter, and R. J. Pettis, "Evaluation of intradermal and subcutaneous infusion set performance under 24-hour basal and bolus conditions," *J Diabetes Sci Technol*, vol. 9, no. 6, pp. 1282–1291, 2015.
13. R. M. Bergenstal, D. C. Klonoff, S. K. Garg, B. W. Bode, M. Meredith, R. H. Slover, A. J. Ahmann, J. B. Welsh, S. W. Lee, and F. R. Kaufman, "Threshold-based insulin-pump interruption for reduction of hypoglycemia," *The N Engl J Med*, vol. 369, no. 3, pp. 224–232, 2013.
14. V. N. Shah, A. Shoskes, B. Tawfik, and S. K. Garg, "Closed-loop system in the management of diabetes: past, present, and future," *Diabetes Technol Ther*, vol. 16, no. 8, pp. 477–490, 2014.
15. N. Baysal, F. Cameron, B. Buckingham, D. M. Wilson, and B. W. Bequette, "Detecting sensor and insulin infusion set anomalies in an artificial pancreas," in *ACC, Washington, DC*, pp. 2929–2933.
16. R. Roberts, J. Walsh, and L. Heinemann, "Help! Someone is beeping," *J Diabetes Sci Technol*, vol. 8, no. 4, pp. 627–629, 2014.
17. J. P. Shivers, L. Mackowiak, H. Anhalt, and H. Zisser, ""'Turn it off!": Diabetes device alarm fatigue considerations for the present and the future," *J Diabetes Sci Technol*, vol. 7, no. 3, pp. 789–794, 2013.
18. E. I. Georga, V. C. Protopappas, C. V. Bellos, and D. I. Fotiadis, "Wearable systems and mobile applications for diabetes disease management," *Health and Technology*, vol. 4, no. 2, pp. 101–112, 2014.
19. A. S. Brazeau, H. Mircescu, K. Desjardins, C. Leroux, I. Strychar, J. M. Ekoe, and R. Rabasa-Lhoret, "Carbohydrate counting accuracy and blood glucose variability in adults with type 1 diabetes," *Diabetes Res Clin Pract*, vol. 99, no. 1, pp. 19–23, 2013.
20. A. C. van Bon, Y. M. Luijf, R. Koebrugge, R. Koops, J. B. L. Hoekstra, and J. H. DeVries, "Feasibility of a portable bihormonal closed-loop system to control glucose excursions at home under free-living conditions for 48 hours," *Diabetes Technol Ther*, vol. 16, no. 3, pp. 131–136, 2014.
21. K. Turksoy, S. Samadi, J. Feng, E. Littlejohn, L. Quinn, and A. Cinar, "Meal detection in patients with type 1 diabetes: A new module for the multivariable adaptive artificial pancreas control system," *IEEE JBHI*, vol. 20, no. 1, pp. 47–54, 2016.
22. G. M. Steil, "Algorithms for a closed-loop artificial pancreas: the case for proportional-integral-derivative control," *J Diabetes Sci Technol*, vol. 7, no. 6, pp. 1621–1631, 2013.

23. B. W. Bequette, "Algorithms for a closed-loop artificial pancreas: The case for model predictive control," *J Diabetes Sci Technol*, vol. 7, no. 6, pp. 1632–1643, 2013.
24. B. W. Bequette, "Fault detection and safety in closed-loop artificial pancreas systems," *J Diabetes Sci Technol*, vol. 8, no. 6, pp. 1204–1214, 2014.
25. Y. Zhang, P. L. Jones, and R. Jetley, "A hazard analysis for a generic insulin infusion pump," *J Diabetes Sci Technol*, vol. 4, no. 2, pp. 263–283, 2010.
26. P. Ross, J. Milburn, D. Reith, E. Wiltshire, and B. Wheeler, "Clinical review: insulin pump-associated adverse events in adults and children," *Acta Diabetol*, vol. 52, no. 6, pp. 1017–1024, 2015.
27. P. Ross, A. Gray, J. Milburn, I. Kumarasamy, F. Wu, S. Farrand, J. Armishaw, E. Wiltshire, J. Rayns, P. Tomlinson, and B. Wheeler, "Insulin pump-associated adverse events are common, but not associated with glycemic control, socio-economic status, or pump/infusion set type," *Acta Diabetologica*, vol. 53, no. 6, pp. 991–998, 2016.
28. I. Rabbone, N. Minuto, S. Toni, F. Lombardo, D. Iafusco, M. Marigliano, R. Schiaffini, G. Maltoni, A. P. Frongia, M. Scardapane, A. Nicolucci, V. Cherubini, R. Bonfanti, and A. E. a. Scaramuzza, "Insulin pump breakdown and infusion set failure in italian children with type 1 diabetes: A 1-year prospective observational study with suggestions to minimize clinical impact," *Diabetes, Obes Metab.*, pp. 1–6, 2018.
29. N. Taleb, V. Messier, S. Ott-Braschi, J.-L. Ardilouze, and R. Rabasa-Lhoret, "Perceptions and experiences of adult patients with type 1 diabetes using continuous subcutaneous insulin infusion therapy: Results of an online survey," *Diabetes Research and Clinical Practice*, vol. 144, pp. 42–50, 2018.
30. I. Guilhem, A. M. Leguerrier, F. Lecordier, J. Y. Poirier, and D. Maugendre, "Technical risks with subcutaneous insulin infusion," *Diabetes Metab*, vol. 32, no. 3, pp. 279–284, 2006.
31. L. Heinemann and L. Krinelke, "Insulin infusion set: the achilles heel of continuous subcutaneous insulin infusion," *J Diabetes Sci Technol*, vol. 6, no. 4, pp. 954–964, 2012.
32. D. Deiss, P. Adolfsson, M. Alkemade-van Zomeren, G. B. Bolli, G. Charpentier, C. Cobelli, T. Danne, A. Girelli, H. Mueller, C. A. Verderese, and E. Renard, "Insulin infusion set use: European perspectives and recommendations," *Diabetes Technol Ther*, vol. 18, no. 9, pp. 517–24, 2016.
33. B. W. Bequette, "Continuous glucose monitoring: real-time algorithms for calibration, filtering, and alarms," *J Diabetes Sci Technol*, vol. 4, no. 2, pp. 404–418, 2010.
34. P. D. Home, "Plasma insulin profiles after subcutaneous injection: how close can we get to physiology in people with diabetes?" *Diabetes Obes Metab*, vol. 17, no. 11, pp. 1011–1020, 2015.
35. C. M. Ramkissoon, J. Veh, B. Aufderheide, B. W. Bequette, and C. C. Palerm, "A taxonomy of safety issues to be overcome in the artificial pancreas," (Abstract No. 445) poster presented at ATTD, Paris, France, 2015.
36. H. Blauw, P. Keith-Hynes, R. Koops, and J. H. DeVries, "A review of safety and design requirements of the artificial pancreas," *Annals of Biomedical Engineering*, pp. 1–15, 2016.
37. C. M. Ramkissoon, B. Aufderheide, B. W. Bequette, and J. Vehi, "A review of safety and hazards associated with the artificial pancreas," *Biomedical Engineering, IEEE Reviews in*, vol. 10, pp. 44–62, 2017.
38. A. J. Kowalski, "Can we really close the loop and how soon? Accelerating the availability of an artificial pancreas: a roadmap to better diabetes outcomes," *Diabetes Technol Ther*, vol. 11, no. S1, pp. S113–S119, 2009.
39. J. Feng, K. Turksoy, and A. Cinar, *Performance Assessment of Model-Based Artificial Pancreas Control Systems*. Springer, 2016, pp. 243–265.
40. A. Guenego, G. Bouzillé, S. Breitel, A. Esvant, J.-Y. Poirier, F. Bonnet, and I. Guilhem, "Insulin pump failures: Has there been an improvement? Update of a prospective observational study," *Diabetes Technol Ther*, vol. 18, no. 12, pp. 820–824, 2016.
41. P. Schaepelynck, P. Darmon, L. Molines, M. Jannot-Lamotte, C. Treglia, and D. Raccah, "Advances in pump technology: insulin patch pumps, combined pumps and glucose sensors, and implanted pumps," *Diabetes Metab*, vol. 37, pp. S85–S93, 2011.
42. A. Liebl, R. Hoogma, E. Renard, P. H. Geelhoed-Duijvestijn, E. Klein, J. Diglas, L. Kessler, V. Melki, P. Diem, J. M. Brun, P. Schaepelynck-Belicar, T. Frei, and G. European DiaPort Study, "A reduction in severe hypoglycaemia in type 1 diabetes in a randomized crossover study of continuous intraperitoneal compared with subcutaneous insulin infusion," *Diabetes Obes Metab*, vol. 11, no. 11, pp. 1001–1008, 2009.

43. M. Blanke, M. Kinnaert, J. Lunze, M. Staroswiecki, and SpringerLink, *Diagnosis and Fault-Tolerant Control*, 2nd ed. Springer Berlin Heidelberg, 2006.
44. S. Vaddiraju, D. J. Burgess, I. Tomazos, F. C. Jain, and F. Papadimitrakopoulos, "Technologies for continuous glucose monitoring: current problems and future promises," *J Diabetes Sci Technol*, vol. 4, no. 6, pp. 1540–1562, 2010.
45. U. Klueh, M. Kaur, Y. Qiao, and D. L. Kreutzer, "Critical role of tissue mast cells in controlling long-term glucose sensor function in vivo," *Biomaterials*, vol. 31, no. 16, pp. 4540–4551, 2010.
46. U. Klueh, O. Antar, Y. Qiao, and D. L. Kreutzer, "Role of vascular networks in extending glucose sensor function: Impact of angiogenesis and lymphangiogenesis on continuous glucose monitoring in vivo," *J Biomed Mater Res A*, vol. 102, no. 10, pp. 3512–3522, 2014.
47. A. El-Laboudi, S. Sharma, N. Oliver, T. Hussein, D. Patel, D. Johnston, and T. Cass, "Development of a novel microprobe array continuous glucose sensor for type 1 diabetes: Interference studies," presented at ATTD, Vienna, Austria, 2014.
48. A. Facchinetti, S. Favero, G. Sparacino, and C. Cobelli, "An online failure detection method of the glucose sensor-insulin pump system: Improved overnight safety of type-1 diabetic subjects," *IEEE Trans. Biomed. Eng.*, vol. 60, no. 2, pp. 406–416, 2013.
49. C. Zhao and Y. Fu, "Statistical analysis based online sensor failure detection for continuous glucose monitoring in type i diabetes," *Chemom. Intell. Lab. Syst.*, vol. 144, pp. 128–137, 2015.
50. U. Klueh, Z. Liu, B. Feldman, T. P. Henning, B. Cho, T. Ouyang, and D. Kreutzer, "Metabolic biofouling of glucose sensors in vivo: role of tissue microhemorrhages," *J Diabetes Sci Technol*, vol. 5, no. 3, pp. 583–595, 2011.
51. U. Klueh, J. T. Frailey, Y. Qiao, O. Antar, and D. L. Kreutzer, "Cell based metabolic barriers to glucose diffusion: macrophages and continuous glucose monitoring," *Biomaterials*, vol. 35, no. 10, pp. 3145–3153, 2014.
52. B. R. King, P. W. Goss, M. A. Paterson, P. A. Crock, and D. G. Anderson, "Changes in altitude cause unintended insulin delivery from insulin pumps mechanisms and implications," *Diabetes Care*, vol. 34, no. 9, pp. 1932–1933, 2011.
53. M. Gibney, Z. Xue, M. Swinney, D. Bialonczyk, and L. Hirsch, "Reduced silent occlusions with a novel catheter infusion set (bd flowsmart): Results from two open-label comparative studies," *Diabetes Technol Ther*, vol. 18, no. 3, pp. 136–143, 2016.
54. D. Kerr, J. Morton, C. Whately-Smith, J. Everett, and J. P. Begley, "Laboratory-based non-clinical comparison of occlusion rates using three rapid-acting insulin analogs in continuous subcutaneous insulin infusion catheters using low flow rates," *J Diabetes Sci Technol*, vol. 2, no. 3, pp. 450–455, 2008.
55. V. Schmid, C. Hohberg, M. Borchert, T. Forst, and A. Pfützner, "Pilot study for assessment of optimal frequency for changing catheters in insulin pump therapy-trouble starts on day 3," *J Diabetes Sci Technol*, vol. 4, no. 4, pp. 976–982, 2010.
56. L. Hojbjerre, C. Skov-Jensen, P. Kaastrup, P. E. Pedersen, and B. Stallknecht, "Effect of steel and teflon infusion catheters on subcutaneous adipose tissue blood flow and infusion counter pressure in humans," *Diabetes Technol Ther*, vol. 11, no. 5, pp. 301–6, 2009.
57. L. Heinemann, "Insulin absorption from lipodystrophic areas: A (neglected) source of trouble for insulin therapy?" *J Diabetes Sci Technol*, vol. 4, no. 3, pp. 750–753, 2010.
58. W. K. Ward, J. R. Castle, and J. El Youssef, "Safe glycemic management during closed-loop treatment of type 1 diabetes: the role of glucagon, use of multiple sensors, and compensation for stress hyperglycemia," *J Diabetes Sci Technol*, vol. 5, no. 6, pp. 1373–1380, 2011.
59. C. Ramkissoon and J. Vehí, *Emotions and Diabetes*, ser. Lecture Notes in Computer Science. Springer International Publishing, 2015, vol. 9044, book section 70, pp. 720–727.
60. M. Salai, I. Vassányi, and I. Kósa, "Stress detection using low cost heart rate sensors," *Journal of Healthcare Engineering*, vol. 2016, 2016.
61. E. Dassau, B. W. Bequette, B. A. Buckingham, and F. J. Doyle, III, "Detection of a meal using continuous glucose monitoring implications for an artificial β-cell," *Diabetes care*, vol. 31, no. 2, pp. 295–300, 2008.
62. H. Lee and B. W. Bequette, "A closed-loop artificial pancreas based on model predictive control: Human-friendly identification and automatic meal disturbance rejection," *Biomed Signal Process Control*, vol. 4, no. 4, pp. 347–354, 2009.

63. H. Lee, B. A. Buckingham, D. M. Wilson, and B. W. Bequette, "A closed-loop artificial pancreas using model predictive control and a sliding meal size estimator," *J Diabetes Sci Technol*, vol. 3, no. 5, p. 1082, 2009.
64. K. Turksoy, A. Roy, and A. Cinar, "Real-time model-based fault detection of continuous glucose sensor measurements," *IEEE Trans. Biomed. Eng.*, 2016.
65. F. Cameron, G. Niemeyer, and B. A. Buckingham, "Probabilistic evolving meal detection and estimation of meal total glucose appearance," *J Diabetes Sci Technol*, vol. 3, no. 5, pp. 1022–1030, 2009.
66. C. S. Hughes, S. D. Patek, M. Breton, and B. P. Kovatchev, "Anticipating the next meal using meal behavioral profiles: A hybrid model-based stochastic predictive control algorithm for t1dm," *Comput Methods Programs Biomed*, vol. 102, no. 2, pp. 138–148, 2011.
67. F. Cameron, G. Niemeyer, and B. W. Bequette, "Extended multiple model prediction with application to blood glucose regulation," *J Process Control*, vol. 22, no. 8, pp. 1422–1432, 2012.
68. M. C. Riddell, D. P. Zaharieva, L. Yavelberg, A. Cinar, and V. K. Jamnik, "Exercise and the development of the artificial pancreas: One of the more difficult series of hurdles," *J Diabetes Sci Technol*, vol. 9, no. 6, pp. 1217–1226, 2015.
69. V. B. Shetty, P. A. Fournier, R. J. Davey, A. J. Retterath, N. Paramalingam, H. C. Roby, M. N. Cooper, E. A. Davis, and T. W. Jones, "Effect of exercise intensity on glucose requirements to maintain euglycaemia during exercise in type 1 diabetes," *J Clin Endocrinol Metab*, pp. jc–2015, 2016.
70. S. Ding and M. Schumacher, "Sensor monitoring of physical activity to improve glucose management in diabetic patients: A review," *Sensors (Basel)*, vol. 16, no. 4, 2016.
71. L. Hinshaw, C. Dalla Man, D. K. Nandy, A. Saad, A. E. Bharucha, J. A. Levine, R. A. Rizza, R. Basu, R. E. Carter, C. Cobelli, Y. C. Kudva, and A. Basu, "Diurnal pattern of insulin action in type 1 diabetes: implications for a closed-loop system," *Diabetes*, vol. 62, no. 7, p. 2223, 2013.
72. N. Baysal, F. Cameron, M. Stenerson, B. Buckingham, D. Wilson, E. Mayer-Davis, D. Maahs, and B. Bequette, "Using activity monitors to improve CGM sensor anomaly detection," in *ATTD, Paris, France*, vol. 15, no. S1, 2013, pp. A2–A2.
73. M. Rausand and A. Høyland, *System Reliability Theory: Models, Statistical Methods, and Applications*, 2nd ed. Wiley, 2004.
74. K. Kölle, A. L. Fougner, S. M. Carlsen, R. Ellingsen, and Ø. Stavdahl, "Failure analysis of an artificial pancreas — double subcutaneous vs. double intraperitoneal approach," (Abstract No. 334) poster presented at ATTD, Milano, Italy, 2016.
75. ISO/TR 12489, *Petroleum, petrochemical and natural gas industries – Reliability modelling and calculation of safety systems*, ISO Standard, 2013.
76. K. Turksoy, L. Quinn, E. Littlejohn, and A. Cinar, "Monitoring and fault detection of continuous glucose sensor measurements," in *ACC, Chicago, US-IL*, 2015, pp. 5091–5096.
77. J. Feng, K. Turksoy, S. Samadi, I. Hajizadeh, and A. Cinar, "Hybrid sensor error detection and functional redundancy for artificial pancreas control systems," in *IFAC DYCOPS-CAB, Trondheim, Norway*, 2016.
78. J. Bondia, C. Tarín, W. García-Gabin, E. Esteve, J. M. Fernández-Real, W. Ricart, and J. Vehí, "Using support vector machines to detect therapeutically incorrect measurements by the MiniMed CGMS®," *J Diabetes Sci Technol*, vol. 2, no. 4, pp. 622–629, 2008.
79. C. Tarin, L. Traver, J. Bondia, and J. Vehí, "A learning system for error detection in subcutaneous continuous glucose measurement using support vector machines," in *CCA, Yokohama, Japan*, 2010, pp. 1614–1619.
80. Y. Leal, M. Ruiz, C. Lorencio, J. Bondia, L. Mujica, and J. Vehi, "Principal component analysis in combination with case-based reasoning for detecting therapeutically correct and incorrect measurements in continuous glucose monitoring systems," *Biomed Signal Process Control*, vol. 8, no. 6, pp. 603–614, 2013.
81. Y. Leal, L. Gonzalez-Abril, C. Lorencio, J. Bondia, and J. Vehi, "Detection of correct and incorrect measurements in real-time continuous glucose monitoring systems by applying a postprocessing support vector machine," *IEEE Trans. Biomed. Eng.*, vol. 60, no. 7, pp. 1891–1899, 2013.
82. F. Cameron, B. Buckingham, D. Wilson, and B. Bequette, "Extending threshold based detection of infusion set failures," presented at DMT, Bethesda, US-MD, 2012.
83. P. Herrero, R. Calm, J. Veh, J. Armengol, P. Georgiou, N. Oliver, and C. Tomazou, "Robust fault detection system for insulin pump therapy using continuous glucose monitoring," *J Diabetes Sci Technol*, vol. 6, no. 5, pp. 1131–1141, 2012.

84. S. Del Favero, M. Monaro, A. Facchinetti, A. Tagliavini, G. Sparacino, and C. Cobelli, "Real-time detection of glucose sensor and insulin pump faults in an artificial pancreas," in *IFAC World Congress, Cape Town, South Africa*, 2014, pp. 1941–1946.
85. D. A. Finan, H. Zisser, L. Jovanovi, D. E. Seborg, and W. C. Bevier, "Automatic detection of stress states in type 1 diabetes subjects in ambulatory conditions," *Industrial and Engineering Chemistry Research*, vol. 49, no. 17, pp. 7843–7848, 2010.
86. R. Rojas, W. Garcia-Gabin, and B. W. Bequette, "Multivariate statistical analysis to detect insulin infusion set failure," in *ACC, San Francisco, US-CA*, 2011, pp. 1952–1957.
87. R. Rojas, W. Garcia-Gabin, and B. W. Bequette, "Mean glucose slope – principal component analysis classification to detect insulin infusion set failure," in *IFAC World Congress, Milano, Italy*, 2011, pp. 14 127–14 132.
88. O. Vega-Hernandez, F. Campos-Cornejo, D. U. Campos-Delgado, and D. R. Espinoza-Trejo, "Increasing security in an artificial pancreas: diagnosis of actuator faults," in *PAHCE, Mexico City, Mexico*, 2009, pp. 137–142.
89. D. P. Howsmon, N. Baysal, B. A. Buckingham, G. P. Forlenza, T. T. Ly, D. M. Maahs, T. Marcal, L. Towers, E. Mauritzen, S. Deshpande, L. M. Huyett, J. E. Pinsker, R. Gondhalekar, I. Francis J. Doyle, E. Dassau, J. Hahn, and B. W. Bequette, "Real-time detection of infusion site failures in a closed-loop artificial pancreas," *Journal of Diabetes Science and Technology*, vol. 12, no. 3, pp. 599–607, 2018.
90. K. Kölle, A. L. Fougner, K. A. F. Unstad, and Ø. Stavdahl, "Fault detection in glucose control: Is it time to move beyond CGM data?" *IFAC-PapersOnLine*, 2018.
91. R. A. Harvey, E. Dassau, H. Zisser, D. E. Seborg, and F. J. Doyle, "Design of the glucose rate increase detector a meal detection module for the health monitoring system," *J Diabetes Sci Technol*, vol. 8, no. 2, pp. 307–320, 2014.
92. K. Turksoy, I. Hajizadeh, S. Samadi, J. Feng, M. Sevil, M. Park, L. Quinn, E. Littlejohn, and A. Cinar, "Real-time insulin bolusing for unannounced meals with artificial pancreas," *Control Engineering Practice*, vol. 59, no. C, pp. 159–164, February 2017.
93. Z. Mahmoudi, K. Nørgaard, N. K. Poulsen, H. Madsen, and J. B. Jørgensen, "Fault and meal detection by redundant continuous glucose monitors and the unscented kalman filter," *Biomedical Signal Processing and Control*, vol. 38, pp. 86–99, 2017.
94. C. M. Ramkissoon, P. Herrero, J. Bondia, and J. Vehi, "Meal detection in the artificial pancreas: Implications during exercise," *IFAC PapersOnLine*, vol. 50, no. 1, pp. 5462–5467, July 2017.
95. C. Ramkissoon, P. Herrero, J. Bondia, and J. Vehi, "Unannounced meals in the artificial pancreas: Detection using continuous glucose monitoring," *Sensors (Switzerland)*, vol. 18, no. 3, 2018.
96. J. Weimer, S. Chen, A. Peleckis, M. R. Rickels, and I. Lee, "Physiology-invariant meal detection for type 1 diabetes," *Diabetes Technology & Therapeutics*, vol. 18, no. 10, pp. 616–624, October 2016.
97. K. Kölle, A. L. Fougner, and Ø. Stavdahl, "Meal detection based on non-individualized moving horizon estimation and classification," in *2017 IEEE Conference on Control Technology and Applications (CCTA)*, Aug 2017, pp. 529–535.
98. S. Samadi, K. Turksoy, I. Hajizadeh, J. Feng, M. Sevil, and A. Cinar, "Meal detection and carbohydrate estimation using continuous glucose sensor data," *Biomedical and Health Informatics, IEEE Journal of*, vol. 21, no. 3, pp. 619–627, May 2017.
99. S. Samadi, M. Rashid, K. Turksoy, J. Feng, I. Hajizadeh, N. Hobbs, C. Lazaro, M. Sevil, E. Littlejohn, and A. Cinar, "Automatic detection and estimation of unannounced meals for multivariable artificial pancreas system," *Diabetes technology & therapeutics*, February 2018.
100. L. Heinemann, G. A. Fleming, J. R. Petrie, R. W. Holl, R. M. Bergenstal, and A. L. Peters, "Insulin pump risks and benefits: A clinical appraisal of pump safety standards, adverse event reporting, and research needs a joint statement of the european association for the study of diabetes and the american diabetes association diabetes technology working group," *Diabetes care*, vol. 38, no. 4, pp. 716–722, 2015.
101. Y. Zhang, R. Jetley, P. L. Jones, and A. Ray, "Generic safety requirements for developing safe insulin pump software," *J Diabetes Sci Technol*, vol. 5, no. 6, pp. 1403–1419, 2011.
102. S. Richter and A. Sereseanu, "Developing effective risk assessment criteria in regulated environments," in *IDAACS, Warsaw, Poland*, vol. 2, 2015, pp. 564–569.
103. S. D. Patek, L. Magni, E. Dassau, C. Hughes-Karvetski, C. Toffanin, G. De Nicolao, S. Del Favero, M. Breton, C. Dalla Man, E. Renard, H. Zisser, F. J. Doyle, III, C. Cobelli, and B. Kovatchev, "Modular closed-loop control of diabetes," *IEEE Trans. Biomed. Eng.*, vol. 59, no. 11, pp. 2986–2999, 2012.

104. V. Venkatasubramanian, R. Rengaswamy, S. Kavuri, and K. Yin, "A review of process fault detection and diagnosis: Part III: Process history based methods," *Comput. Chem. Eng.*, vol. 27, no. 3, pp. 327–346, 2003.
105. N. Baysal, F. Cameron, B. A. Buckingham, D. M. Wilson, H. P. Chase, D. M. Maahs, B. W. Bequette, T. Aye, P. Clinton, and B. P. Harris, "A novel method to detect pressure-induced sensor attenuations (PISA) in an artificial pancreas," *J Diabetes Sci Technol*, vol. 8, no. 6, pp. 1091–1096, 2014.
106. J. R. Castle, A. Pitts, K. Hanavan, R. Muhly, J. El Youssef, C. Hughes-Karvetski, B. Kovatchev, and W. K. Ward, "The accuracy benefit of multiple amperometric glucose sensors in people with type 1 diabetes," *Diabetes care*, vol. 35, no. 4, pp. 706–710, 2012.
107. R. Shah, J. Kristensen, K. Wolfe, S. Aasmul, and A. Bansal, "Orthogonally redundant sensor systems and methods," US Generic US20 130 060 105 A1, 2013.
108. F. J. Doyle, III, L. M. Huyett, J. B. Lee, H. C. Zisser, and E. Dassau, "Closed-loop artificial pancreas systems: engineering the algorithms," *Diabetes Care*, vol. 37, no. 5, pp. 1191–1197, 2014.
109. D. Howsmon and B. W. Bequette, "Hypo- and hyperglycemic alarms devices and algorithms," *J Diabetes Sci Technol*, vol. 9, no. 5, pp. 1126–1137, 2015.
110. J. Walsh, R. Roberts, R. Morris, and L. Heinemann, "Device connectivity the next big wave in diabetes," *J Diabetes Sci Technol*, vol. 9, no. 3, pp. 701–705, 2015.
111. ISO 14155, *Clinical investigation of medical devices for human subjects – Good clinical practice*, ISO Standard, 2011.
112. C. Cobelli, E. Renard, and B. Kovatchev, "Artificial pancreas: past, present, future," *Diabetes*, vol. 60, no. 11, pp. 2672–2682, 2011.
113. R. Isermann and P. Ball, "Trends in the application of model-based fault detection and diagnosis of technical processes," *Control Engineering Practice*, vol. 5, no. 5, pp. 709–719, 1997.
114. IEC 60050, *International Electrotechnical Vocabulary*, IEC Standard.
115. IEC 61508-4, *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems. Part 4: Definitions and Abbreviations*, IEC Standard, 2010.